PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-152014
(43)Date of publication of application : 27.05.2004

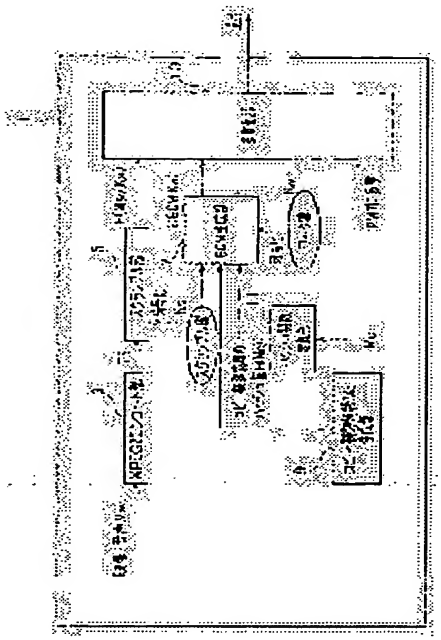
(51)Int.Cl. G06F 12/14
H04L 9/08
H04N 7/173

(21)Application number : 2002-316508
(22)Date of filing : 30.10.2002

(71)Applicant : NIPPON HOSO KYOKAI <NHK>
(72)Inventor : NISHIMOTO TOMONARI
BABA AKITSUGU
KURIOKA TATSUYA

(54) CONTENTS TRANSMITTING METHOD, CONTENTS TRANSMITTING DEVICE, CONTENTS TRANSMITTING PROGRAM, CONTENTS RECEIVING METHOD, CONTENTS RECEIVING DEVICE, AND CONTENTS RECEIVING PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a contents transmitting method, device and program and a contents receiving method, device and program capable of preventing the illicit copying of contents.
SOLUTION: This contents transmitting device 1 transmits copy control information that is the information for controlling the copying frequency of the contents on a receiver side after receiving the contents with the contents. This device 1 has a scramble part 5 for encrypting the contents with a first encryption key to form encrypted contents, a hash function arithmetic part 11 for arithmetically operating the copy control information with a hash function and processing it to a hash value, an ECM generation part 7 for encrypting related information including the first encryption key and the function arithmetic information with a second encryption key to form first encryption key related information, and a multiplexing part 13 for multiplexing the encrypted contents, the copy control information and the first encryption key related information followed by transmitting.



LEGAL STATUS

[Date of request for examination] 10.03.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-152014
(P2004-152014A)
(43)公開日　平成16年5月27日(2004.5.27)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 12/14	G06F 12/14	320E	5B017
H04L 9/08	G06F 12/14	310Z	5C064
H04N 7/173	H04N 7/173	640Z	5J104
	H04L 9/00	601B	

審査請求 未請求　請求項の数 8　OL　（全 26 頁）

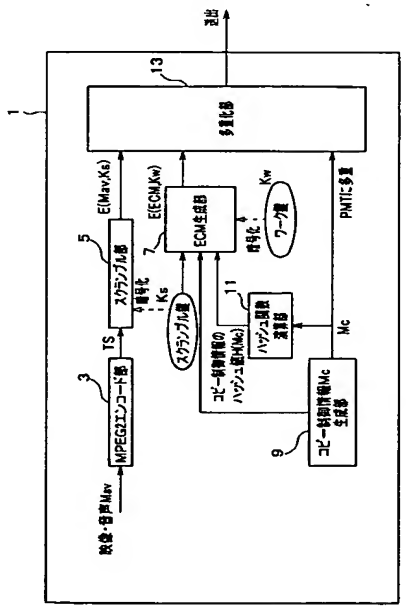
(21)出願番号　特願2002-316508(P2002-316508)
(22)出願日　平成14年10月30日(2002.10.30)

(71)出願人　000004352
日本放送協会
東京都渋谷区神南２丁目２番１号
(74)代理人　100064414
弁理士　磯野　道造
(72)発明者　西本　友成
東京都世田谷区砧一丁目１０番１１号　日本放送協会　放送技術研究所内
(72)発明者　馬場　秋緒
東京都世田谷区砧一丁目１０番１１号　日本放送協会　放送技術研究所内

最終頁に続く

(54)【発明の名称】コンテンツ送信方法、コンテンツ送信装置、コンテンツ送信プログラムおよびコンテンツ受信方法、コンテンツ受信装置、コンテンツ受信プログラム

(57)【要約】
【課題】コンテンツの不正コピーの防止をすることができるコンテンツ送信、装置、プログラムおよびコンテンツ受信方法、装置、プログラムを提供する。
【解決手段】コンテンツを受信した後、この受信側において当該コンテンツをコピーする回数を制御する情報であるコピー制御情報を当該コンテンツと共に送信するコンテンツ送信装置１であって、コンテンツを第一暗号鍵で暗号化して暗号化コンテンツとするスクランブル部５と、コピー制御情報をハッシュ関数で演算し、ハッシュ値に加工するハッシュ関数演算部１１と、第一暗号鍵を含む関連情報および前記関数演算情報を第二暗号鍵で暗号化して、第一暗号鍵関連情報とするＥＣＭ生成部７と、暗号化コンテンツ、コピー制御情報および第一暗号鍵関連情報を多重化して送出する多重化部１３と、を備えた。
【選択図】　図１



【特許請求の範囲】
【請求項１】
コンテンツをコピーする回数を制御する情報であるコピー制御情報を当該コンテンツと共に送信するコンテンツ送信方法であって、
前記コンテンツを第一暗号鍵で暗号化して暗号化コンテンツとするコンテンツ暗号化ステップと、
前記コピー制御情報を所定関数で演算した関数演算情報に加工するコピー制御情報加工ステップと、
前記第一暗号鍵を含む関連情報および前記関数演算情報を第二暗号鍵で暗号化して、第一暗号鍵関連情報とする第一暗号鍵暗号化ステップと、
前記暗号化コンテンツ、前記コピー制御情報および前記第一暗号鍵関連情報を多重化した多重暗号化コンテンツとして送出する多重送出ステップと、
を含むことを特徴とするコンテンツ送信方法。
【請求項２】
コンテンツをコピーする回数を制御する情報であるコピー制御情報を当該コンテンツと共に送信するコンテンツ送信装置であって、
前記コンテンツを第一暗号鍵で暗号化して暗号化コンテンツとするコンテンツ暗号化手段と、
前記コピー制御情報を所定関数で演算した関数演算情報に加工するコピー制御情報加工手段と、
前記第一暗号鍵を含む関連情報および前記関数演算情報を第二暗号鍵で暗号化して、第一暗号鍵関連情報とする第一暗号鍵暗号化手段と、
前記暗号化コンテンツ、前記コピー制御情報および前記第一暗号鍵関連情報を多重化した多重暗号化コンテンツとして送出する多重送出手段と、
を備えることを特徴とするコンテンツ送信装置。
【請求項３】
コンテンツをコピーする回数を制御する情報であるコピー制御情報を当該コンテンツと共に送信するコンテンツ送信装置であって、
前記コンテンツを第一暗号鍵で暗号化して暗号化コンテンツとするコンテンツ暗号化手段と、
前記コピー制御情報を含む前記コンテンツの利用全般に係る情報である利用条件情報を所定関数で演算した関数演算情報に加工するコピー制御情報加工手段と、
前記第一暗号鍵を含む関連情報および前記関数演算情報を第二暗号鍵で暗号化して、第一暗号鍵関連情報とする第一暗号鍵暗号化手段と、
前記暗号化コンテンツ、前記利用条件情報および前記第一暗号鍵関連情報を多重化した多重暗号化コンテンツとして送出する多重送出手段と、
を備えることを特徴とするコンテンツ送信装置。
【請求項４】
コンテンツをコピーする回数を制御する情報であるコピー制御情報を当該コンテンツと共に送信する装置を、
前記コンテンツを第一暗号鍵で暗号化して暗号化コンテンツとするコンテンツ暗号化手段、
前記コピー制御情報を所定関数で演算した関数演算情報に加工するコピー制御情報加工手段、
前記第一暗号鍵を含む関連情報および前記関数演算情報を第二暗号鍵で暗号化して、第一暗号鍵関連情報とする第一暗号鍵暗号化手段、
前記暗号化コンテンツ、前記コピー制御情報および前記第一暗号鍵関連情報を多重化した多重暗号化コンテンツとして送出する多重送出手段、
として機能させることを特徴とするコンテンツ送信プログラム。
【請求項５】

請求項１記載のコンテンツ送信方法によって送信された多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されているコピー制御情報が改ざんされていない場合に、当該コンテンツを利用可能にするコンテンツ受信方法であって、
前記多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されている暗号化コンテンツおよびコピー制御情報と、第一暗号鍵関連情報とを分離する受信分離ステップと、
この受信分離ステップにて分離された第一暗号鍵関連情報を、送信側に備えられている第二暗号鍵と同様の第二暗号鍵で復号化し、第一暗号鍵関連情報に含まれている第一暗号鍵および関数演算情報を取得する第一暗号鍵関連情報復号化ステップと、
前記受信分離ステップにて分離された暗号化コンテンツおよびコピー制御情報からコピー制御情報を抽出し、前記送信側に備えられている所定関数と同様の所定関数で当該コピー制御情報を演算し、比較用関数演算情報とする演算ステップと、
前記第一暗号鍵関連情報復号ステップにて取得された関数演算情報と、前記演算ステップにて演算された比較用関数演算情報とを比較し、前記関数演算情報に加工する前の原文データであるコピー制御情報が改ざんされているか否かを判定する関数演算情報比較ステップと、
この関数演算情報比較ステップにおける比較結果に基づいて、前記第一暗号鍵の送出を制御する第一暗号鍵送出制御ステップと、
この第一暗号鍵送出制御ステップにおいて送出された第一暗号鍵で、前記暗号化コンテンツを復号化して出力するコンテンツ復号化出力ステップと、
を含むことを特徴とするコンテンツ受信方法。
【請求項６】
請求項２記載のコンテンツ送信装置によって送信された多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されているコピー制御情報が改ざんされていない場合に、当該コンテンツを利用可能にするコンテンツ受信装置であって、
前記多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されている暗号化コンテンツおよびコピー制御情報と、第一暗号鍵関連情報とを分離する受信分離手段と、
この受信分離手段で分離された第一暗号鍵関連情報を、送信側に備えられている第二暗号鍵と同様の第二暗号鍵で復号化し、第一暗号鍵関連情報に含まれている第一暗号鍵および関数演算情報を取得する第一暗号鍵関連情報復号化手段と、
前記受信分離手段で分離された暗号化コンテンツおよびコピー制御情報からコピー制御情報を抽出し、前記送信側に備えられている所定関数と同様の所定関数で当該コピー制御情報を演算し、比較用関数演算情報とする演算手段と、
前記第一暗号鍵関連情報復号化手段で取得された関数演算情報と、前記演算手段で演算された比較用関数演算情報とを比較し、前記関数演算情報に加工する前の原文データであるコピー制御情報が改ざんされているか否かを判定する関数演算情報比較手段と、
この関数演算情報比較手段における比較結果に基づいて、前記第一暗号鍵の送出を制御する第一暗号鍵送出制御手段と、この第一暗号鍵送出制御手段で送出された第一暗号鍵で、前記暗号化コンテンツを復号化して出力するコンテンツ復号化出力手段と、
を備えることを特徴とするコンテンツ受信装置。
【請求項７】
請求項３記載のコンテンツ送信装置によって送信された多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されているコピー制御情報が改ざんされていない場合に、当該コンテンツを利用可能にするコンテンツ受信装置であって、
前記多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されている暗号化コンテンツと、利用条件情報と、第一暗号鍵関連情報とを分離する受信分離手段と、
この受信分離手段で分離された第一暗号鍵関連情報を、送信側に備えられている第二暗号鍵と同様の第二暗号鍵で復号化し、第一暗号鍵関連情報に含まれている第一暗号鍵および関数演算情報を取得する第一暗号鍵関連情報復号化手段と、

前記受信分離手段で分離された利用条件情報を、前記送信側に備えられている所定関数と同様の所定関数で当該利用条件情報を演算し、比較用関数演算情報とする演算手段と、
前記第一暗号鍵関連情報復号化手段で取得された関数演算情報と、前記演算手段で演算された比較用関数演算情報とを比較し、前記関数演算情報に加工する前の原文データであるコピー制御情報が改ざんされているか否かを判定する関数演算情報比較手段と、
前記利用条件情報に基づいて、暗号化コンテンツを復号化可能か判定する判定結果を出力する利用判定手段と、
前記関数演算情報比較手段における比較結果および前記利用判定手段における判定結果に基づいて、前記第一暗号鍵の送出を制御する第一暗号鍵送出制御手段と、
この第一暗号鍵送出制御手段で送出された第一暗号鍵で、前記暗号化コンテンツを復号化して出力するコンテンツ復号化出力手段と、
を備えることを特徴とするコンテンツ受信装置。

【請求項８】

請求項４記載のコンテンツ送信プログラムによって送信された多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されているコピー制御情報が改ざんされていない場合に、当該コンテンツを利用可能にする装置を、
前記多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されている暗号化コンテンツおよびコピー制御情報と、第一暗号鍵関連情報とを分離する受信分離手段、
この受信分離手段で分離された第一暗号鍵関連情報を、送信側に備えられている第二暗号鍵と同様の第二暗号鍵で復号化し、第一暗号鍵関連情報に含まれている第一暗号鍵および関数演算情報を取得する第一暗号鍵関連情報復号化手段、
前記受信分離手段で分離された暗号化コンテンツおよびコピー制御情報からコピー制御情報を抽出し、前記送信側に備えられている所定関数と同様の所定関数で当該コピー制御情報を演算し、比較用関数演算情報とする演算手段、
前記第一暗号鍵関連情報復号化手段で取得された関数演算情報と、前記演算手段で演算された比較用関数演算情報とを比較し、前記関数演算情報に加工する前の原文データであるコピー制御情報が改ざんされているか否かを判定する関数演算情報比較手段、
この関数演算情報比較手段における比較結果に基づいて、前記第一暗号鍵の送出を制御する第一暗号鍵送出制御手段、
この第一暗号鍵送出制御手段で送出された第一暗号鍵で、前記暗号化コンテンツを復号化して出力するコンテンツ復号化出力手段、
として機能させることを特徴とするコンテンツ受信プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、コンテンツ、特にデジタルコンテンツの権利管理保護の一環である不正コピーを防止して送信または受信するコンテンツ送信方法、コンテンツ送信装置、コンテンツ送信プログラムおよびコンテンツ受信方法、コンテンツ受信装置、コンテンツ受信プログラムに関する。

【０００２】

【従来の技術】

従来、コンテンツ（特に、デジタルコンテンツ）を送受信するデジタル放送システムにおいて、当該デジタルコンテンツを受信するデジタル放送受信装置は、受信したデジタルコンテンツに含まれるＰＭＴ（Ｐｒｏｇｒａｍ　ＭａＰ　Ｔａｂｌｅ）等にデジタルコピー制御記述子として多重化されているコピー制御情報に従って、当該受信装置に備えられている（付属している）蓄積装置（或いは、他の記憶媒体）へのデジタルコンテンツのコピー制御を行っている。

【０００３】

このデジタル放送システムにおいて、特に、限定受信方式（例えば、非特許文献１参照）

の場合であっても、デジタルコンテンツ（映像、音声）はトランスポートストリームパケットにエンコード（符号化）後、暗号化（スクランブル）されるが、ＰＭＴは暗号化されておらず、デジタルコピー制御記述子（コピー制御情報）は平文（符号化または暗号化されていない情報）の状態で伝送されている。

【０００４】

【非特許文献１】

電波産業会（ＡＲＩＢ）の標準規格「デジタル放送に使用する番組配列情報」（ＡＲＩＢ　ＳＴＤ－Ｂ１０）、Ｐ１０８、Ｐ１４７

【０００５】

【発明が解決しようとする課題】

しかしながら、従来のデジタル放送システムにおいて、デジタルコピー制御記述子（コピー制御情報）を不正に改ざんして、例えば、デジタルコンテンツのデジタルコピー制御記述子（コピー制御情報）が「コピー禁止」となっているのを「コピー自由」にして、蓄積装置（他の記憶媒体）に蓄積することで不正コピーされる恐れが生じるという問題がある。

【０００６】

そこで、本発明の目的は前記した従来の技術が有する課題を解消し、コンテンツの不正コピーの防止をすることができるコンテンツ送信方法、コンテンツ送信装置、コンテンツ送信プログラムおよびコンテンツ受信方法、コンテンツ受信装置、コンテンツ受信プログラムを提供することにある。

【０００７】

【課題を解決するための手段】

本発明は、前記した目的を達成するため、以下に示す構成とした。

請求項１記載のコンテンツ送信方法は、コンテンツをコピーする回数を制御する情報であるコピー制御情報を当該コンテンツと共に送信するコンテンツ送信方法であって、前記コンテンツを第一暗号鍵で暗号化して暗号化コンテンツとするコンテンツ暗号化ステップと、前記コピー制御情報を所定関数で演算した関数演算情報に加工するコピー制御情報加工ステップと、前記第一暗号鍵を含む関連情報および前記関数演算情報を第二暗号鍵で暗号化して、第一暗号鍵関連情報とする第一暗号鍵暗号化ステップと、前記暗号化コンテンツ、前記コピー制御情報および前記第一暗号鍵関連情報を多重化した多重暗号化コンテンツとして送出する多重送出ステップと、を含むことを特徴とする。

【０００８】

この方法によれば、まず、コンテンツ暗号化ステップにおいて、コンテンツが第一暗号鍵で暗号化され、暗号化コンテンツとされる。また、コピー制御情報加工ステップにおいて、コピー制御情報が所定関数で演算され、関数演算情報に加工される。所定関数とは、この場合、ある情報Ａを当該所定関数で演算した結果、この情報Ａのデータ量を縮小させると共に、解読不能にするもので、例えば、ハッシュ関数が挙げられる。そして、第一暗号鍵暗号化ステップにおいて、第一暗号鍵および関数演算情報が第二暗号鍵で暗号化され、第一暗号鍵関連情報とされる。その後、多重送出ステップにおいて、暗号化コンテンツ、コピー制御情報および第一暗号鍵関連情報が多重化され送出される。

【０００９】

なお、第一暗号鍵を含む関連情報とは、第一暗号鍵と、コンテンツを提供した事業者ＩＤ、つまり放送局、コンテンツ制作会社等の識別情報を含む情報である。

【００１０】

また、通常、受信側の限定した受信者のみが視聴できるように、送信側でコンテンツを処理することを「スクランブルする」というが、ここでは、「暗号化する」という文言で統一的に表現している。

【００１１】

さらに、第一暗号鍵は、例えば、経過時間と共に数秒単位で変更されるスクランブル鍵を指すものであり、第二暗号鍵は、例えば、コンテンツの継続時間よりも長時間保持される

ワーク鍵を指すものである。

【００１２】

請求項２記載のコンテンツ送信装置は、コンテンツをコピーする回数を制御する情報であるコピー制御情報を当該コンテンツと共に送信するコンテンツ送信装置であって、前記コンテンツを第一暗号鍵で暗号化して暗号化コンテンツとするコンテンツ暗号化手段と、前記コピー制御情報を所定関数で演算した関数演算情報に加工するコピー制御情報加工手段と、前記第一暗号鍵を含む関連情報および前記関数演算情報を第二暗号鍵で暗号化して、第一暗号鍵関連情報とする第一暗号鍵暗号化手段と、前記暗号化コンテンツ、前記コピー制御情報および前記第一暗号鍵関連情報を多重化した多重暗号化コンテンツとして送出する多重送出手段と、を備えることを特徴とする。

【００１３】

かかる構成によれば、コンテンツ暗号化手段で、コンテンツが第一暗号鍵で暗号化され、暗号化コンテンツとされる。また、コピー制御情報加工手段で、コピー制御情報が所定関数で演算され、関数演算情報に加工される。そして、第一暗号鍵暗号化手段で、第一暗号鍵および関数演算情報が第二暗号鍵で暗号化され、第一暗号鍵関連情報とされる。その後、多重送出手段で、暗号化コンテンツ、コピー制御情報および第一暗号鍵関連情報が多重化され送出される。

【００１４】

請求項３記載のコンテンツ送信装置は、コンテンツをコピーする回数を制御する情報であるコピー制御情報を当該コンテンツと共に送信するコンテンツ送信装置であって、前記コンテンツを第一暗号鍵で暗号化して暗号化コンテンツとするコンテンツ暗号化手段と、前記コピー制御情報を含む前記コンテンツの利用全般に係る情報である利用条件情報を所定関数で演算した関数演算情報に加工するコピー制御情報加工手段と、前記第一暗号鍵を含む関連情報および前記関数演算情報を第二暗号鍵で暗号化して、第一暗号鍵関連情報とする第一暗号鍵暗号化手段と、前記暗号化コンテンツ、前記利用条件情報および前記第一暗号鍵関連情報を多重化した多重暗号化コンテンツとして送出する多重送出手段と、を備えることを特徴とする。

【００１５】

かかる構成によれば、コンテンツ暗号化手段で、コンテンツが第一暗号鍵で暗号化され、暗号化コンテンツとされる。また、コピー制御情報加工手段で、コピー制御情報を含む利用条件情報が所定関数で演算され、関数演算情報に加工される。そして、第一暗号鍵暗号化手段で、第一暗号鍵および関数演算情報が第二暗号鍵で暗号化され、第一暗号鍵関連情報とされる。その後、多重送出手段で、暗号化コンテンツ、利用条件情報および第一暗号鍵関連情報が多重化され送出される。なお、利用条件情報は、通常、汎用的なＸＭＬ言語等で記述されており、コピー制御情報に比べ、データ量が格段に多いので、多重送出手段で多重化する前にＤＳＭ－ＣＣデータカルーセル等を用いた上で、暗号化コンテンツおよび第一暗号鍵関連情報に多重化される。また、ＤＳＭ－ＣＣデータカルーセルは、データ放送等に使用されるダウンロードデータカルーセルのことである。

【００１６】

請求項４記載のコンテンツ送信プログラムは、コンテンツをコピーする回数を制御する情報であるコピー制御情報を当該コンテンツと共に送信する装置を、以下に示す手段として機能させることを特徴とする。当該装置を機能させる手段は、前記コンテンツを第一暗号鍵で暗号化して暗号化コンテンツとするコンテンツ暗号化手段、前記コピー制御情報を所定関数で演算した関数演算情報に加工するコピー制御情報加工手段、前記第一暗号鍵を含む関連情報および前記関数演算情報を第二暗号鍵で暗号化して、第一暗号鍵関連情報とする第一暗号鍵暗号化手段、前記暗号化コンテンツ、前記コピー制御情報および前記第一暗号鍵関連情報を多重化した多重暗号化コンテンツとして送出する多重送出手段、である。

【００１７】

かかる構成によれば、コンテンツ暗号化手段で、コンテンツが第一暗号鍵で暗号化され、暗号化コンテンツとされる。また、コピー制御情報加工手段で、コピー制御情報が所定関

数で演算され、関数演算情報に加工される。そして、第一暗号鍵暗号化手段で、第一暗号鍵および関数演算情報が第二暗号鍵で暗号化され、第一暗号鍵関連情報とされる。その後、多重送出手段で、暗号化コンテンツ、コピー制御情報および第一暗号鍵関連情報が多重化され送出される。

【００１８】

請求項５記載のコンテンツ受信方法は、請求項１記載のコンテンツ送信方法によって送信された多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されているコピー制御情報が改ざんされていない場合に、当該コンテンツを利用可能にするコンテンツ受信方法であって、前記多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されている暗号化コンテンツおよびコピー制御情報と、第一暗号鍵関連情報とを分離する受信分離ステップと、この受信分離ステップにて分離された第一暗号鍵関連情報を、送信側に備えられている第二暗号鍵と同様の第二暗号鍵で復号化し、第一暗号鍵関連情報に含まれている第一暗号鍵および関数演算情報を取得する第一暗号鍵関連情報復号化ステップと、前記受信分離ステップにて分離された暗号化コンテンツおよびコピー制御情報からコピー制御情報を抽出し、前記送信側に備えられている所定関数と同様の所定関数で当該コピー制御情報を演算し、比較用関数演算情報とする演算ステップと、前記第一暗号鍵関連情報復号ステップにて取得された関数演算情報と、前記コピー制御情報演算ステップにて演算された比較用関数演算情報とを比較し、前記関数演算情報に加工する前の原文データであるコピー制御情報が改ざんされているか否かを判定する関数演算情報比較ステップと、この関数演算情報比較ステップにおける比較結果に基づいて、前記第一暗号鍵の送出を制御する第一暗号鍵送出制御ステップと、この第一暗号鍵送出制御ステップにおいて送出された第一暗号鍵で、前記暗号化コンテンツを復号化して出力するコンテンツ復号化出力ステップと、を含むことを特徴とする。

【００１９】

この方法によれば、まず、受信分離ステップにおいて、受信された多重暗号化コンテンツが暗号化コンテンツおよびコピー制御情報と、第一暗号鍵関連情報とに分離される。続いて、第一暗号鍵関連情報復号化ステップにおいて、第一暗号鍵関連情報が第二暗号鍵で復号化され、この第一暗号鍵関連情報に含まれている第一暗号鍵および関数演算情報が取得される。演算ステップにおいて、送信側に備えられている所定関数と同様の所定関数で、コピー制御情報が演算され、比較用関数演算情報とされる。関数演算情報比較ステップにおいて、関数演算情報と比較用関数演算情報とが比較され、この比較結果に基づき、第一暗号鍵送出制御ステップにおいて、第一暗号鍵の送出が制御される。その後、コンテンツ復号化出力ステップにおいて、暗号化コンテンツが第一暗号鍵で復号化されて出力される。

【００２０】

なお、受信分離ステップにおいて、暗号化コンテンツおよびコピー制御情報と、第一暗号鍵関連情報とに分離されるのは、第一暗号鍵関連情報のみを、記憶されている情報が外部から読取不可能なセキュリティモジュール内で扱うためである。

【００２１】

ここでは、便宜上、第一暗号鍵および第二暗号鍵で復号化されるといった表現を使用しているが、実際には、第一暗号鍵および第二暗号鍵は、例えば、スクランブル鍵、ワーク鍵等と表現されるものである。

【００２２】

請求項６記載のコンテンツ受信装置は、請求項２記載のコンテンツ送信装置によって送信された多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されているコピー制御情報が改ざんされていない場合に、当該コンテンツを利用可能にするコンテンツ受信装置であって、前記多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されている暗号化コンテンツおよびコピー制御情報と、第一暗号鍵関連情報とを分離する受信分離手段と、この受信分離手段で分離された第一暗号鍵関連情報を、送信側に備えられている第二暗号鍵と同様の第二暗号鍵で復号化し、第一暗号鍵関連情報に含ま

れている第一暗号鍵および関数演算情報を取得する第一暗号鍵関連情報復号化手段と、前記受信分離手段で分離された暗号化コンテンツおよびコピー制御情報からコピー制御情報を抽出し、前記送信側に備えられている所定関数と同様の所定関数で当該コピー制御情報を演算し、比較用関数演算情報とする演算手段と、前記第一暗号鍵関連情報復号化手段で取得された関数演算情報と、前記演算手段で演算された比較用関数演算情報とを比較し、前記関数演算情報に加工する前の原文データであるコピー制御情報が改ざんされているか否かを判定する関数演算情報比較手段と、この関数演算情報比較手段における比較結果に基づいて、前記第一暗号鍵の送出を制御する第一暗号鍵送出制御手段と、この第一暗号鍵送出制御手段で送出された第一暗号鍵で、前記暗号化コンテンツを復号化して出力するコンテンツ復号化出力手段と、を備えることを特徴とする。

【００２３】

かかる構成によれば、受信分離手段で、受信された多重暗号化コンテンツが暗号化コンテンツおよびコピー制御情報と、第一暗号鍵関連情報とに分離される。続いて、第一暗号鍵関連情報復号化手段で、第一暗号鍵関連情報が第二暗号鍵で復号化され、この第一暗号鍵関連情報に含まれている第一暗号鍵および関数演算情報が取得される。演算手段で、送信側に備えられている所定関数と同様の所定関数で、コピー制御情報が演算され、比較用関数演算情報とされる。関数演算情報比較手段で、関数演算情報と比較用関数演算情報とが比較され、この比較結果に基づき、第一暗号鍵送出制御手段で、第一暗号鍵の送出が制御される。その後、コンテンツ復号化出力手段で、暗号化コンテンツが第一暗号鍵で復号化されて出力される。

【００２４】

請求項７記載のコンテンツ受信装置は、請求項８記載のコンテンツ送信装置によって送信された多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されているコピー制御情報が改ざんされていない場合に、当該コンテンツを利用可能にするコンテンツ受信装置であって、前記多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されている暗号化コンテンツと、利用条件情報と、第一暗号鍵関連情報とを分離する受信分離手段と、この受信分離手段で分離された第一暗号鍵関連情報を、送信側に備えられている第二暗号鍵と同様の第二暗号鍵で復号化し、第一暗号鍵関連情報に含まれている第一暗号鍵および関数演算情報を取得する第一暗号鍵関連情報復号化手段と、前記受信分離手段で分離された利用条件情報を、前記送信側に備えられている所定関数と同様の所定関数で当該利用条件情報を演算し、比較用関数演算情報とする演算手段と、前記第一暗号鍵関連情報復号化手段で取得された関数演算情報と、前記演算手段で演算された比較用関数演算情報とを比較し、前記関数演算情報に加工する前の原文データであるコピー制御情報が改ざんされているか否かを判定する関数演算情報比較手段と、前記利用条件情報に基づいて、暗号化コンテンツを復号化可能か判定し、判定した判定結果を出力する利用判定手段と、前記関数演算情報比較手段における比較結果および前記利用判定手段における判定結果に基づいて、前記第一暗号鍵の送出を制御する第一暗号鍵送出制御手段と、この第一暗号鍵送出制御手段で送出された第一暗号鍵で、前記暗号化コンテンツを復号化して出力するコンテンツ復号化出力手段と、を備えることを特徴とする。

【００２５】

かかる構成によれば、受信分離手段で、受信された多重暗号化コンテンツが暗号化コンテンツと、利用条件情報と、第一暗号鍵関連情報とに分離される。続いて、第一暗号鍵関連情報復号化手段で、第一暗号鍵関連情報が第二暗号鍵で復号化され、この第一暗号鍵関連情報に含まれている第一暗号鍵および関数演算情報が取得される。演算手段で、送信側に備えられている所定関数と同様の所定関数で、利用条件情報が演算され、比較用関数演算情報とされる。関数演算情報比較手段で、関数演算情報と比較用関数演算情報とが比較され、利用判定手段で、暗号化コンテンツが復号化可能か判定され、これら比較結果、判定結果に基づき、第一暗号鍵送出制御手段で、第一暗号鍵の送出が制御される。その後、コンテンツ復号化出力手段で、暗号化コンテンツが第一暗号鍵で復号化されて出力される。

【００２６】

なお、利用条件情報は、受信後、蓄積装置等に蓄積させた場合のコンテンツの視聴有効期間や、再生可能回数、再生可能時間、早送り再生等の特殊再生の可否（ＣＭとばし等）、ノンリニア再生の可否等の、受信側でコンテンツを利用する際の条件となる詳細な制御情報のことである。また、所定関数の演算は、外部から記憶されている情報が読取不可能なセキュリティモジュール等の内部で行われる。

【００２７】

請求項８記載のコンテンツ受信プログラムは、請求項４記載のコンテンツ送信プログラムによって送信された多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されているコピー制御情報が改ざんされていない場合に、当該コンテンツを利用可能にする装置を、以下に示す手段として機能させることを特徴とする。当該装置を機能させる手段は、前記多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されている暗号化コンテンツおよびコピー制御情報と、第一暗号鍵関連情報とを分離する受信分離手段、この受信分離手段で分離された第一暗号鍵関連情報を、送信側に備えられている第二暗号鍵と同様の第二暗号鍵で復号化し、第一暗号鍵関連情報に含まれている第一暗号鍵および関数演算情報を取得する第一暗号鍵関連情報復号化手段、前記受信分離手段で分離された暗号化コンテンツおよびコピー制御情報からコピー制御情報を抽出し、前記送信側に備えられている所定関数と同様の所定関数で当該コピー制御情報を演算し、比較用関数演算情報とする演算手段、前記第一暗号鍵関連情報復号化手段で取得された関数演算情報と、前記演算手段で演算された比較用関数演算情報とを比較し、前記関数演算情報に加工する前の原文データであるコピー制御情報が改ざんされているか否かを判定する関数演算情報比較手段、この関数演算情報比較手段における比較結果に基づいて、前記第一暗号鍵の送出を制御する第一暗号鍵送出制御手段、この第一暗号鍵送出制御手段で送出された第一暗号鍵で、前記暗号化コンテンツを復号化して出力するコンテンツ復号化出力手段、である。

【００２８】

かかる構成によれば、受信分離手段で、受信された多重暗号化コンテンツが暗号化コンテンツおよびコピー制御情報と、第一暗号鍵関連情報とに分離される。続いて、第一暗号鍵関連情報復号化手段で、第一暗号鍵関連情報が第二暗号鍵で復号化され、この第一暗号鍵関連情報に含まれている第一暗号鍵および関数演算情報が取得される。演算手段で、コピー制御情報が送信側に備えられている所定関数と同様の所定関数で演算され、比較用関数演算情報とされる。関数演算情報比較手段で、関数演算情報と比較用関数演算情報とが比較され、この比較結果に基づき、第一暗号鍵送出制御手段で、第一暗号鍵の送出が制御される。その後、コンテンツ復号化出力手段で、暗号化コンテンツが第一暗号鍵で復号化されて出力される。

【００２９】

【発明の実施の形態】

以下、本発明の一実施の形態について、図面を参照して詳細に説明する。

（コンテンツ送信装置の構成：第一の実施形態）

図１に示すコンテンツ送信装置のブロック図を参照して、コンテンツ送信装置（第一の実施の形態）の構成について説明する。図１に示すように、コンテンツ送信装置１は、ＭＰＥＧ２エンコード部３と、スクランブル部５と、ＥＣＭ生成部７と、コピー制御情報Ｍｃ生成部９と、ハッシュ関数演算部１１と、多重化部１３とを備えている。

【００３０】

コンテンツ送信装置１は、コンテンツ（デジタルコンテンツ、以下、コンテンツに統一して表記する）を受信した受信側で、利用する（再生する）際にコピー（複製）の制御を可能にして当該コンテンツを送信するものである。

【００３１】

ＭＰＥＧ２エンコード部３は、入力された映像音声コンテンツである映像音声Ｍａｖ（コンテンツ）を符号化（エンコード）して、ＭＰＥＧ２形式の映像音声コンテンツストリーム（ＴＳ）を生成するものである。なお、エンコードとは、映像音声信号からデジタル符

号を生成することであり、エンコードの目的は、アナログ信号をデジタル信号に変換することや、デジタル信号の冗長度を減らすことで、元の信号を圧縮して伝送または蓄積されるデータ量を減少させること等が挙げられる。

【００３２】

スクランブル部５は、ＭＰＥＧ２エンコード部３でエンコードされた映像音声コンテンツストリーム（ＴＳ）をスクランブル鍵ＫＳでスクランブルして、暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））を生成するものである。このコンテンツ送信装置１には、スクランブル鍵ＫＳを生成するスクランブル鍵生成手段（図示せず）が備えられている。スクランブルは、ストリーム形式の信号の暗号化を指すものであり、スクランブル鍵ＫＳは、コンテンツの経過時間に伴い、数秒単位（一般的には１秒程度）で変更される暗号鍵である。なお、このスクランブル部５が特許請求の範囲の請求項に記載したコンテンツ暗号化手段に相当するものであり、スクランブル鍵ＫＳが第一暗号鍵に相当するものである。

【００３３】

ＥＣＭ生成部７は、スクランブル鍵ＫＳを含む関連情報と、ハッシュ関数演算部１１で演算されたハッシュ値Ｈ（Ｍｃ）とをワーク鍵Ｋｗで暗号化して、受信側で映像音声ＭａＶを再生する時に用いられる第一暗号鍵関連情報（Ｅ（ＥＣＭ．Ｋｗ））を生成するものである。スクランブル鍵ＫＳを含む関連情報とは、スクランブル鍵ＫＳと、コンテンツを提供した事業者ＩＤ、つまり放送局、コンテンツ制作会社等の識別情報を含む情報のことである。ハッシュ値Ｈ（Ｍｃ）は、原文データ（元々の情報、原文、或いは、平文ともいう）をハッシュ関数（後記する）で演算した生成データであり、この生成データから原文データを推定することが不可能なものである。ハッシュ値Ｈ（Ｍｃ）が特許請求の範囲の請求項に記載した関数演算情報に相当するものである。

【００３４】

第一暗号鍵関連情報は、いわゆるＥＣＭ（Ｅｎｔｉｔｌｅｍｅｎｔ Ｃｏｎｔｒｏｌ Ｍｅｓｓａｇｅ：共通情報）であり、この第一暗号鍵関連情報（Ｅ（ＥＣＭ．Ｋｗ））は、受信側のコンテンツ受信装置（後記する）で暗号化コンテンツを復号化する際に用いられるものである。ワーク鍵Ｋｗは、送信側であるコンテンツ送信装置１と受信側であるコンテンツ受信装置（後記する）との間で、長期間にわたり共通に保持される暗号鍵である。ＥＣＭは、コンテンツに関する情報やデスクランブルを行うための鍵情報等から構成され、暗号化された暗号箇所と暗号化されていない非暗号箇所とを含んでなるものである。なお、ワーク鍵Ｋｗが特許請求の範囲の請求項に記載した第二暗号鍵に相当するものである。

【００３５】

コピー制御情報Ｍｃ生成部９は、コンテンツ送信者側（放送局側、コンテンツ制作者側）の意図に応じたコピー制御情報Ｍｃを生成するものであり、このコピー制御情報Ｍｃは、例えば、「コピー禁止」、「コピー一世代可（コピー１回可能）」、「コピー自由」といったように、受信側にてコンテンツのコピー（複製）を制御するための情報である。なお、このコピー制御情報Ｍｃは数十バイトのバイナリの情報である。

【００３６】

ハッシュ関数演算部１１は、コピー制御情報Ｍｃ生成部９で生成されたコピー制御情報Ｍｃをハッシュ関数で演算し、ハッシュ値Ｈ（Ｍｃ）を生成し、ＥＣＭ生成部７に出力するものである。ハッシュ関数は、任意の長さの原文データを固定長の生成データに圧縮するための関数であって、例えば、ＳＨＡ－１や、ＭＤ５というハッシュ関数が代表的なもので、これらＳＨＡ－１およびＭＤ５は、双方とも一方向関数であり、生成データから原文データの推測を不可能にするものである。なお、このハッシュ関数演算部１１が特許請求の範囲の請求項に記載したコピー制御情報加工手段に相当するものであり、ハッシュ値Ｈ（Ｍｃ）が特許請求の範囲の請求項に記載した関数演算情報に相当するものである。

【００３７】

多重化部１３は、暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））と、第一暗号鍵関連情報（Ｅ（ＥＣＭ．Ｋｗ））と、コピー制御情報とを多重化した多重暗号化コンテンツをＭＰＥＧ

２トランスポートストリーム形式で送出するものである。また、この多重化部１３は、図示を省略したデータ放送コンテンツも多重暗号化コンテンツに多重して、送出することができる。なお、コピー制御情報Ｍｃは、映像音声コンテンツストリーム（ＴＳ）のＰＭＴ（Ｐｒｏｇｒａｍ　ＭａＰ　Ｔａｂｌｅ）に多重化されている。また、この多重化部１３が特許請求の範囲の請求項に記載した多重送出手段に相当するものである。

【００３８】

このコンテンツ送信装置１によれば、スクランブル部５で、映像音声コンテンツストリーム（ＴＳ）がスクランブル鍵ＫＳでスクランブルされ、暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））とされる。また、コピー制御情報Ｍｃ生成部９で生成されたコピー制御情報Ｍｃがハッシュ関数演算部１１で演算され、ハッシュ値Ｈ（Ｍｃ）が生成される。そして、ＥＣＭ生成部７で、スクランブル鍵ＫＳを含む関連情報と、コピー制御情報Ｍｃのハッシュ値Ｈ（Ｍｃ）とがワーク鍵Ｋｗで暗号化され、第一暗号鍵関連情報（Ｅ（ＥＣＭ．Ｋｗ））とされる。その後、多重化部１３で、暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））と、第一暗号鍵関連情報（Ｅ（ＥＣＭ．Ｋｗ））と、コピー制御情報Ｍｃとが多重化されて多重暗号化コンテンツとして出力される。

【００３９】

このため、受信側にて、多重暗号化コンテンツに多重化されているハッシュ値Ｈ（Ｍｃ）と、受信側で送信側のハッシュ関数演算部１１に備えられるハッシュ関数と同様のハッシュ関数でコピー制御情報Ｍｃが演算されて得られたハッシュ値Ｈ（Ｍｃ）とが比較されれば、この比較結果に基づいて、映像音声Ｍａｖ（コンテンツ）が利用可能かどうかを判定することができる。

【００４０】

つまり、比較結果により、多重化されていたハッシュ値Ｈ（Ｍｃ）と受信側で演算したハッシュ値Ｈ（Ｍｃ）とが一致した場合、コピー制御情報Ｍｃが改ざんされていないことになり、映像音声Ｍａｖ（コンテンツ）の利用が許可される。また、多重化されていたハッシュ値Ｈ（Ｍｃ）と受信側で演算したハッシュ値Ｈ（Ｍｃ）とが一致しない場合、コピー制御情報Ｍｃが改ざんされたことになり、映像音声Ｍａｖ（コンテンツ）の利用が不許可とされる。

【００４１】

これにより、映像音声Ｍａｖ（コンテンツ）の不正コピーの防止、または、不正なコピー制御情報を含む映像音声Ｍａｖ（コンテンツ）の生成を防止することができる。

【００４２】

（コンテンツ受信装置の構成：第一の実施の形態）

次に、図２に示すコンテンツ受信装置のブロック図を参照して、コンテンツ受信装置（第一の実施の形態）の構成について説明する。この図２に示すように、コンテンツ受信装置２１は、受信分離部２３と、コピー制御情報Ｍｃ抽出部２５と、ハッシュ関数演算部２７と、セキュリティモジュール２９と、デスクランブル部３７と、ＭＰＥＧ２デコード部３９と、コンテンツ蓄積部４１とを備えている。

【００４３】

コンテンツ受信装置２１は、送信側のコンテンツ送信装置１（図１参照）から送信された多重暗号化コンテンツを受信し、この多重暗号化コンテンツに多重化されているコピー制御情報Ｍｃを送信側のコンテンツ送信装置１に備えられているハッシュ関数で演算して、当該多重暗号化コンテンツに多重化されているハッシュ値Ｈ（Ｍｃ）と比較することで、コピー制御情報Ｍｃが改ざんされていないことを検出し、これに基づいて、暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））をデスクランブルして利用するものである。例えば、このコンテンツ受信装置２１でデスクランブルされた映像音声Ｍａｖをディスプレイ（ＴＶ等）に出力したり、多重化されているコピー制御情報Ｍｃに基づいて、当該映像音声Ｍａｖを蓄積したりすることができる。

【００４４】

受信分離部２３は、送信側のコンテンツ送信装置１から送信された多重暗号化コンテンツ

を受信して、暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））およびコピー制御情報Ｍｃと、第一暗号鍵関連情報（Ｅ（ＥＣＭ．Ｋｗ））とを分離し、暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））およびコピー制御情報Ｍｃをコピー制御情報Ｍｃ抽出部２５に出力すると共に、第一暗号鍵関連情報（Ｅ（ＥＣＭ．Ｋｗ））をセキュリティモジュール２９に出力するものである。つまり、この受信分離部２３では、受信したＭＰＥＧ２トランスポートストリームのパケット（多重暗号化コンテンツ）をフィルタリングして、映像音声パケット（暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））およびコピー制御情報Ｍｃ）と、ＥＣＭパケット（第一暗号鍵関連情報（Ｅ（ＥＣＭ．Ｋｗ））とに分離する。なお、この受信分離部２３が特許請求の範囲の請求項に記載した受信分離手段に相当するものである。

【００４５】

コピー制御情報Ｍｃ抽出部２５は、受信分離部２３で分離された暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））およびコピー制御情報Ｍｃから、コピー制御情報Ｍｃを抽出して、ハッシュ関数演算部２７と外部の蓄積装置（図示せず）に出力すると共に、暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））およびコピー制御情報Ｍｃをデスクランブル部３７に出力するものである。つまり、このコピー制御情報Ｍｃ抽出部２５は、コピー制御情報Ｍｃを外部に出力することにより、外部の蓄積装置等で映像音声Ｍａｖを再暗号化してから、当該コピー制御情報Ｍｃに基づいて再暗号化した映像音声Ｍａｖを取り扱えるようにしている。

【００４６】

また、コピー制御情報Ｍｃは、暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））のＰＭＴ部に記憶されている（含まれている）ので、分離させずにデスクランブル部３７に出力される。また、外部の蓄積装置（図示せず）は、例えば、Ｄ－ＶＨＳ等であり、コピー制御情報Ｍｃ抽出部２５で抽出されたコピー制御情報Ｍｃは、ＩＥＥＥ１３９４等のホームネットワークを介して、当該蓄積装置に出力される。

【００４７】

なお、このコピー制御情報Ｍｃ抽出部２５でコピー制御情報Ｍｃが抽出され、不正に改ざんされた場合、セキュリティモジュール２９内の送出制御部３５でスクランブル鍵ＫＳの送出が停止されるため、スクランブルされている暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））をデスクランブルできない。つまり、不正に改ざんされたコピー制御情報Ｍｃに基づいてコンテンツ蓄積部４１に、暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））がスクランブルされたまま蓄積されることになって、映像音声Ｍａｖ（コンテンツ）を不正利用することができない。

【００４８】

また、ＩＥＥＥ１３９４等のホームネットワークを介して、外部の蓄積装置（図示せず）にコピー制御情報Ｍｃを蓄積する場合も同様に、不正に改ざんされたコピー制御情報Ｍに基づいて、ＩＥＥＥ１３９４の伝送保護技術であるＤＴＣＰで暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））が伝送される（送出される）がスクランブルされたままＤＴＣＰで保護されるため、映像音声Ｍａｖ（コンテンツ）を不正利用することができない。補足しておくと、この実施の形態では、多重暗号化コンテンツのＰＭＴの部分に、コピー制御情報Ｍｃを暗号化せずに平文のまま、多重して送信する既存の送出方法で送出しているので、既存のコンテンツ受信装置に悪影響を及ぼすことはない。

【００４９】

ハッシュ関数演算部２７は、コピー制御情報Ｍｃ抽出部２５で抽出されたコピー制御情報Ｍｃをハッシュ関数で演算し、ハッシュ値Ｈ（Ｍｃ）を生成してセキュリティモジュール２９に出力するものである。このハッシュ関数演算部２７で使用されるハッシュ関数は、送信側のコンテンツ送信装置１のハッシュ関数演算部１１に備えられるハッシュ関数と同一のものであり、このハッシュ関数演算部２７で演算されたハッシュ値Ｈ（Ｍｃ）が特許請求の範囲の請求項に記載した比較用関数演算情報に相当するものである。このハッシュ関数演算部２７で演算されたハッシュ値Ｈ（Ｍｃ）を以下、比較用ハッシュ値Ｈ（Ｍｃ）と記載することにする。このハッシュ関数演算部２７が特許請求の範囲の請求項に記載した演算手段に相当するものである。

【００５０】
セキュリティモジュール２９は、ＩＣカード等によって構成され、内部に記録した情報が外部より読取不可能に構成されており、耐タンパー性（耐衝撃性）を備えたモジュールであり、ＥＣＭ解析部３１と、比較部３３と、送出制御部３５とを備えている。
【００５１】
ＥＣＭ解析部３１は、第一暗号鍵関連情報（Ｅ（ＥＣＭ．Ｋｗ））を、予め送信側のコンテンツ送信装置１と受信側のコンテンツ受信装置２１とで共通に保持されているワーク鍵Ｋｗで復号化して、スクランブル鍵ＫＳと、コピー制御情報Ｍｃのハッシュ値Ｈ（Ｍｃ）とを取得し、スクランブル鍵ＫＳを送出制御部３５に出力すると共に、ハッシュ値Ｈ（Ｍｃ）を比較部３３に出力するものである。このＥＣＭ解析部３１が特許請求の範囲の請求項に記載した第一暗号鍵関連情報復号化手段に相当するものである。
【００５２】
比較部３３は、ＥＣＭ解析部３１で取得されたハッシュ値Ｈ（Ｍｃ）と、ハッシュ関数演算部２７で演算された比較用ハッシュ値Ｈ（Ｍｃ）とを比較して、一致していた場合、送出制御部３５にスクランブル鍵ＫＳ送出許可信号を出力すると共に、一致していない場合、送出制御部３５にスクランブル鍵ＫＳ送出不可信号を出力するものである。スクランブル鍵ＫＳ送出許可信号は、送出制御部３５からセキュリティモジュール２９の外部にスクランブル鍵ＫＳの出力を許可する信号で、スクランブル鍵ＫＳ送出不可信号は、送出制御部３５からセキュリティモジュール２９の外部にスクランブル鍵ＫＳの出力を不可にする信号である。
【００５３】
なお、この比較部３３が特許請求の範囲の請求項に記載した関数演算情報比較手段に相当するものであり、これらスクランブル鍵ＫＳ送出許可信号およびスクランブル鍵ＫＳ送出不可信号が特許請求の範囲の請求項に記載した比較結果に相当するものである。
【００５４】
送出制御部３５は、比較部３３から出力されたスクランブル鍵ＫＳ送出許可信号またはスクランブル鍵ＫＳ送出不可信号に基づいて、ＥＣＭ解析部３１から入力されたスクランブル鍵ＫＳの出力を制御するものである。この送出制御部３５が特許請求の範囲の請求項に記載した第一暗号鍵送出制御手段に相当するものである。
【００５５】
デスクランブル部３７は、暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））をセキュリティモジュール２９の送出制御部３５から出力されたスクランブル鍵ＫＳでデスクランブルして、ＭＰＥＧ２形式の映像音声コンテンツストリーム（ＴＳ）を生成するものである。
【００５６】
ＭＰＥＧ２デコード部３９は、デスクランブル部３７から出力されたＭＰＥＧ２形式の映像音声コンテンツストリーム（ＴＳ）をデコードした映像音声Ｍａｖをコンテンツ受信装置２１の外部に備えられる表示装置（図示せず）に送出するものである。なお、デスクランブル部３７およびＭＰＥＧ２デコード部３９が特許請求の範囲の請求項に記載したコンテンツ復号化出力手段に相当するものである。
【００５７】
コンテンツ蓄積部４１は、大容量のハードディスク等によって構成され、コピー制御情報Ｍｃ抽出部２５から出力された暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））を蓄積すると共に、デスクランブル部３７でデスクランブルされた映像音声Ｍａｖ（コンテンツ）を蓄積するものである。但し、コピー制御情報Ｍｃ抽出部２５で抽出されたコピー制御情報Ｍｃが「コピー禁止」であれば、デスクランブルされた映像音声Ｍａｖ（コンテンツ）を蓄積することができず、この旨を通知するメッセージ（「コピー禁止のコンテンツであるので蓄積できません！」等のメッセージ）が図示を省略した表示部に表示される。
【００５８】
このコンテンツ受信装置２１によれば、受信分離部２３で、受信された多重暗号化コンテンツが暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））およびコピー制御情報Ｍｃと、第一暗号

鍵関連情報（Ｅ（ＥＣＭ．Ｋｗ））とに分離される。続いて、ＥＣＭ解析部３１で、第一暗号鍵関連情報（Ｅ（ＥＣＭ．Ｋｗ））がワーク鍵Ｋｗで復号化され、この第一暗号鍵関連情報（Ｅ（ＥＣＭ．Ｋｗ））に含まれているスクランブル鍵ＫＳおよびハッシュ値Ｈ（Ｍｃ）が取得される。ハッシュ関数演算部２７で、送信側のコンテンツ送信装置１に備えられている ハッシュ関数と同様のハッシュ関数で、コピー制御情報Ｍｃが演算され、比較用ハッシュ値Ｈ（Ｍｃ）とされる。比較部３３で、ハッシュ値Ｈ（Ｍｃ）と比較用ハッシュ値Ｈ（Ｍｃ）とが比較され、この比較結果に基づき、送出制御部３５で、スクランブル鍵ＫＳの送出が制御される。その後、デスクランブル部３７で、暗号化コンテンツ（Ｅ（ＭａＶ．ＫＳ））がスクランブル鍵ＫＳで復号化され、ＭＰＥＧ２デコード部３９でデコードされ、映像音声ＭａＶ（コンテンツ）として出力される。

【００５９】

このため、多重暗号化コンテンツに多重化されているハッシュ値Ｈ（Ｍｃ）と、送信側のハッシュ関数演算部１１に備えられるハッシュ関数と同様のハッシュ関数でコピー制御情報Ｍｃが演算されて得られた比較用ハッシュ値Ｈ（Ｍｃ）とが比較され、この比較結果に基づいて、映像音声ＭａＶ（コンテンツ）が利用可能かどうかを判定することができる。

【００６０】

つまり、比較結果により、多重化されていたハッシュ値Ｈ（Ｍｃ）と演算して得られた比較用ハッシュ値Ｈ（Ｍｃ）とが一致した場合、コピー制御情報Ｍｃが改ざんされていないことになり、映像音声ＭａＶ（コンテンツ）の利用が許可される。また、多重化されていたハッシュ値Ｈ（Ｍｃ）と受信側で演算したハッシュ値Ｈ（Ｍｃ）とが一致しない場合、コピー制御情報Ｍｃが改ざんされたことになり、映像音声ＭａＶ（コンテンツ）の利用が不許可とされる。これにより、映像音声ＭａＶ（コンテンツ）の不正コピーの防止、または、不正なコピー制御情報を含む映像音声ＭａＶ（コンテンツ）の生成を防止することができる。

【００６１】

なお、このコンテンツ受信装置２１では、ハッシュ関数演算部２７でコピー制御情報Ｍｃをハッシュ関数で演算して、比較用ハッシュ値Ｈ（Ｍｃ）を生成して、比較部３３でハッシュ値Ｈ（Ｍｃ）と比較用ハッシュ値Ｈ（Ｍｃ）とを比較したが、予め、送信側のコンテンツ送信装置１において、第一暗号鍵関連情報（ＥＥＣＭ．Ｋｗ）にハッシュ値Ｈ（Ｍｃ）を含めるのではなくコピー制御情報Ｍｃを含めておき、セキュリティモジュール２９内の比較部３３で、コピー制御情報Ｍｃ同士を比較してもよい。

【００６２】

ただし、コピー制御情報Ｍｃは、映像、音声、データなどのコンポーネント毎に付与することができ、数十バイトに膨れ上がる可能性があるため、送信側のコンテンツ送信装置１において、ハッシュ関数で演算してハッシュ値Ｈ（Ｍｃ）を生成した方が、ＥＣＭ生成部７でＥ（ＥＣＭ．Ｋｗ）のデータ量を小さく生成することができ、放送伝送帯域を効率的に利用することができる。また、この実施の形態では、ハッシュ関数演算部２７をセキュリティモジュール２９の外部に設けたが、このハッシュ関数演算部２７をセキュリティモジュール２９の内部に設けてもよい。

【００６３】

（コンテンツ送信装置の動作：第一の実施の形態）

次に、図３に示すフローチャートを参照して、コンテンツ送信装置の動作を説明する（適宜図１参照）。

まず、コンテンツ送信装置１のＭＰＥＧ２エンコード部３に映像音声ＭａＶ（コンテンツ）が入力され、このＭＰＥＧ２エンコード部３で映像音声ＭａＶ（コンテンツ）がエンコードされて、ＭＰＥＧ２形式の映像音声コンテンツストリーム（ＴＳ）とされスクランブル部５へ出力される（Ｓ１）。

【００６４】

続いて、スクランブル部５で映像音声コンテンツストリーム（ＴＳ）がスクランブル鍵ＫＳでスクランブルされて、暗号化コンテンツ（Ｅ（ＭａＶ．ＫＳ））とされ、多重化部１

３へ出力される（Ｓ２）。このスクランブル部５で使用されたスクランブル鍵ＫＳに当該スクランブル鍵ＫＳに関する情報が付加されて、スクランブル鍵ＫＳを含む関連情報とされ、このスクランブル鍵ＫＳを含む関連情報がＥＣＭ生成部７に入力される。

【００６５】

また、コピー制御情報Ｍｃ生成部９でコピー制御情報Ｍｃが生成され、ハッシュ関数演算部１１と多重化部１３へ出力される（Ｓ３）。なお、コピー制御情報Ｍｃは、多重化部１３においてＰＭＴに多重化される。すると、ハッシュ関数演算部１１でコピー制御情報Ｍｃが当該ハッシュ関数演算部１１に備えられているハッシュ関数によって演算され、ハッシュ値Ｈ（Ｍｃ）とされてＥＣＭ生成部７へ出力される（Ｓ４）。

【００６６】

そして、ＥＣＭ生成部７で、スクランブル鍵ＫＳを含む関連情報とハッシュ値Ｈ（Ｍｃ）とがワーク鍵Ｋｗで暗号化され、第一暗号鍵関連情報（Ｅ（ＥＣＭ，Ｋｗ））とされて多重化部１３に出力される（Ｓ５）。その後、多重化部１３で暗号化コンテンツ（Ｅ（Ｍａｖ，ＫＳ））、第一暗号鍵関連情報（Ｅ（ＥＣＭ，Ｋｗ））およびコピー制御情報Ｍｃ（ＰＭＴとして）が多重化され、多重暗号化コンテンツとされて、送出される（Ｓ６）。

【００６７】

（コンテンツ受信装置の動作：第一の実施の形態）

次に、図４、図５に示すフローチャートを参照して、コンテンツ受信装置２１の動作を説明する（適宜図２参照）。なお、このコンテンツ受信装置２１の動作の説明では、送信側のコンテンツ送信装置１から送信された多重暗号化コンテンツを受信した後、コピー制御情報Ｍｃが改ざんされているか否かにより、映像音声Ｍａｖ（コンテンツ）を再生するまでの概略を説明したものである。また、このコンテンツ受信装置２１の動作の説明では、多重暗号化コンテンツを復号化またはデスクランブルにかかる情報のみに言及して説明している。

【００６８】

送信側のコンテンツ送信装置１から送出された多重暗号化コンテンツが、コンテンツ受信装置２１の受信分離部２３で受信される（Ｓ１１）。すると、受信分離部２３で多重暗号化コンテンツが分離され、暗号化コンテンツ（Ｅ（Ｍａｖ，ＫＳ））およびコピー制御情報Ｍｃがコピー制御情報Ｍｃ抽出部２５へ出力されると共に、第一暗号鍵関連情報（Ｅ（ＥＣＭ，Ｋｗ））がＥＣＭ解析部３１へ出力される（Ｓ１２）。

【００６９】

そして、コピー制御情報Ｍｃ抽出部２５でコピー制御情報Ｍｃが抽出され、ハッシュ関数演算部２７と外部の蓄積装置（図示せず）等へ出力されると共に、暗号化コンテンツ（Ｅ（Ｍａｖ，ＫＳ））およびコピー制御情報Ｍｃがデスクランブル部３７へ出力される（Ｓ１３）。すると、ハッシュ関数演算部２７でコピー制御情報Ｍｃがハッシュ関数で演算され、比較用ハッシュ値Ｈ（Ｍｃ）が生成され、比較部３３へ出力される（Ｓ１４）。また、ＥＣＭ解析部３１で第一暗号鍵関連情報（Ｅ（ＥＣＭ，Ｋｗ））がワーク鍵Ｋｗで復号化され、ハッシュ値Ｈ（Ｍｃ）およびスクランブル鍵ＫＳが取得され、ハッシュ値Ｈ（Ｍｃ）が比較部３３へ出力されると共に、スクランブル鍵ＫＳが送出制御部３５へ出力される（Ｓ１５）。これより図５を参照する。

【００７０】

そして、比較部３３でハッシュ値Ｈ（Ｍｃ）と比較用ハッシュ値Ｈ（Ｍｃ）とが比較され、一致するか否かが判定される（Ｓ１６）。つまり、このＳ１６にて、比較部３３でハッシュ値Ｈ（Ｍｃ）と比較用ハッシュ値Ｈ（Ｍｃ）とが比較された結果（比較結果）によって、コピー制御情報Ｍｃが改ざんされたか否かが判断できる。すなわち、比較結果が一致していれば、改ざんされていないと判断でき、一致していなければ、改ざんされていると判断できる。

【００７１】

この比較部３３でハッシュ値Ｈ（Ｍｃ）と比較用ハッシュ値Ｈ（Ｍｃ）とが一致すると判定された場合（Ｓ１６、ＹｅＳ）、比較部３３からスクランブル鍵ＫＳ送出許可信号（図

中、許可信号）が送出制御部３５へ出力される（Ｓ１７）。送出制御部３５で、スクランブル鍵ＫＳ送出許可信号に基づいて、スクランブル鍵ＫＳがデスクランブル部３７へ出力される（Ｓ１８）。デスクランブル部３７で暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））がデスクランブルされ、ＭＰＥＧ２形式の映像音声コンテンツストリーム（ＴＳ）が得られ、ＭＰＥＧ２デコード部３９に出力される（Ｓ１９）。ＭＰＥＧ２デコード部３９で、ＭＰＥＧ２形式の映像音声コンテンツストリーム（ＴＳ）がデコードされ映像音声Ｍａｖ（コンテンツ）が出力される（Ｓ２０）。

【００７２】

また、Ｓ１６にて、ハッシュ値Ｈ（Ｍｃ）と比較用ハッシュ値Ｈ（Ｍｃ）とが一致しないと判定された場合（Ｓ１６、Ｎｏ）、比較部３３からスクランブル鍵ＫＳ送出不可信号（図中、不可信号）が送出制御部３５へ出力され（Ｓ２１）、暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））を再生できない旨のメッセージが図示を省力した表示部に表示される（Ｓ２２）。

【００７３】

（コンテンツ送信装置の構成：第二の実施形態）

図６は、図１に示したコンテンツ送信装置１の別の実施の形態（第二の実施の形態）であるコンテンツ送信装置１Ａのブロック図であり、この図６を参照して、コンテンツ送信装置１Ａの構成を説明する。なお、コンテンツ送信装置１の構成と同一の構成は、同一の符号を付してその説明を省略する。

【００７４】

図６に示したこのコンテンツ送信装置１Ａはマークアップ記述言語型利用条件情報Ｍｍｌ生成部５１を備えており、このマークアップ記述言語型利用条件情報Ｍｍｌ生成部５１は、ＸＭＬ（ｅＸｔｅｎｓｉｂｌｅ　ＭａｒｋｕＰ　Ｌａｎｇｕａｇｅ）等のマークアップ記述言語で記述された、コンテンツの利用条件を規定した利用条件情報Ｍｍｌを生成するものである。この利用条件情報Ｍｍｌは、コピー制御情報Ｍｃを含んでおり、その他にも受信側で蓄積した映像音声Ｍａｖ（コンテンツ）の視聴有効期間や、再生可能回数、再生可能時間、早送り再生等の特殊再生の可否、ノンリニア再生（不連続再生）の可否等の映像音声Ｍａｖ（コンテンツ）の利用に関する詳細な制御情報である。

【００７５】

ＸＭＬは汎用的なコンピュータ言語（マークアップ記述言語）であり、様々な端末機器（例えば、後記するコンテンツ受信装置２１Ａ）で利用することができる。また、映像音声Ｍａｖ（コンテンツ）の利用条件情報Ｍｍｌにマークアップ記述言語を用いると、バイナリで記述するよりもデータサイズ（データ量）が大きくなるため、コピー制御情報Ｍｃ単独の場合とは異なり、ＰＭＴ等に多重化することが困難である。このため、この実施の形態では、利用条件情報ＭｍｌはＤＳＭ－ＣＣデータカルーセル（Ｄｉｇｉｔａｌ　Ｓｔｏｒａｇｅ　Ｍｅｄｉａ　Ｃｏｍｍａｎｄ　ａｎｄ　Ｃｏｎｔｒｏｌ：ダウンロードカルーセル方式）等を用いて多重化する。

【００７６】

このコンテンツ送信装置１Ａによれば、スクランブル部５で、映像音声コンテンツストリーム（ＴＳ）がスクランブル鍵ＫＳでスクランブルされ、暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））とされる。また、マークアップ記述言語型利用条件情報Ｍｍｌ生成部５１で生成された利用条件情報Ｍｍｌがハッシュ関数演算部１１で演算され、ハッシュ値Ｈ（Ｍｍｌ）が生成される。そして、ＥＣＭ生成部７で、スクランブル鍵ＫＳを含む関連情報と、利用条件情報Ｍｍｌのハッシュ値Ｈ（Ｍｍｌ）とがワーク鍵Ｋｗで暗号化され、第一暗号鍵関連情報（Ｅ（ＥＣＭ．Ｋｗ））とされる。その後、多重化部１３で、暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））と、第一暗号鍵関連情報（Ｅ（ＥＣＭ．Ｋｗ））と、利用条件情報Ｍｍｌとが多重化されて多重暗号化コンテンツとして出力される。

【００７７】

このため、受信側にて、多重暗号化コンテンツに多重化されているハッシュ値Ｈ（Ｍｍｌ）と、受信側で送信側のハッシュ関数演算部１１に備えられるハッシュ関数と同様のハッ

シュ関数で利用条件情報Ｍｍｉが演算されて得られたハッシュ値Ｈ（Ｍｍｉ）とが比較され、さらに利用条件情報Ｍｍｉに基づいて、暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））を復号化可能かが判定されれば、これら比較結果および判定結果に基づいて、映像音声Ｍａｖ（コンテンツ）が利用可能かどうかを判定することができる。

【００７８】

つまり、比較結果により、多重化されていたハッシュ値Ｈ（Ｍｍｉ）と受信側で演算したハッシュ値Ｈ（Ｍｍｉ）とが一致した場合、利用条件情報Ｍｍｉに含まれているコピー制御情報Ｍｃが改ざんされていないことになり、さらに利用条件情報Ｍｍｉで示される各条件に合致していれば、映像音声Ｍａｖ（コンテンツ）の利用が許可される。また、多重化されていたハッシュ値Ｈ（Ｍｍｉ）と受信側で演算したハッシュ値Ｈ（Ｍｍｉ）とが一致しない場合、利用条件情報Ｍｍｉに含まれているコピー制御情報Ｍｃが改ざんされたことになり、または、利用条件情報Ｍｍｉで示される各条件に合致していなければ、映像音声Ｍａｖ（コンテンツ）の利用が不許可とされる。これにより、映像音声Ｍａｖ（コンテンツ）の不正コピーの防止、または、不正なコピー制御情報を含む映像音声Ｍａｖ（コンテンツ）の生成を防止することができる。

【００７９】

（コンテンツ受信装置の構成：第二の実施の形態）

図７は、図２に示したコンテンツ受信装置２１の別の実施の形態（第二の実施の形態）であるコンテンツ受信装置２１Ａのブロック図であり、この図７を参照して、コンテンツ受信装置２１Ａの構成を説明する。なお、コンテンツ送信装置２１の構成と同一の構成は、同一の符号を付してその説明を省略する。

【００８０】

図７に示したコンテンツ受信装置２１Ａは、利用条件情報Ｍｍｉ抽出部６１と、セキュリティモジュール２９Ａに利用判定部６３と備えている。利用条件情報Ｍｍｉ抽出部６１は、受信分離部２３で分離されたＤＳＭ－ＣＣデータカルーセルから利用条件情報Ｍｍｉを抽出して、セキュリティモジュール２９Ａの利用判定部６３および外部の蓄積装置（図示せず）に出力するものである。

【００８１】

利用判定部６３は、利用条件情報Ｍｍｉに含まれている各条件を判定するもので、各条件を満たしていると判定された場合、映像音声Ｍａｖ利用許可信号が送出制御部３５に出力され、各条件を満たしていると判定されない場合、映像音声Ｍａｖ利用不可信号が送出制御部３５に出力される。例えば、映像音声Ｍａｖ（コンテンツ）の利用有効期限を過ぎている（超過している）場合や、映像音声Ｍａｖ（コンテンツ）の再生時間を過ぎている（超過している）場合等は、映像音声Ｍａｖ（コンテンツ）が利用不可能であると判定され（各条件を満たしていると判定されない）、映像音声Ｍａｖ利用不可信号が送出制御部３５に出力される。

【００８２】

このコンテンツ受信装置２１Ａによれば、受信分離部２３で、受信された多重暗号化コンテンツが暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））と、ＤＳＭ－ＣＣデータカルーセル（利用条件情報Ｍｍｉ）と、第一暗号鍵関連情報（Ｅ（ＥＣＭ．Ｋｗ））とに分離される。続いて、ＥＣＭ解析部３１で、第一暗号鍵関連情報（Ｅ（ＥＣＭ．Ｋｗ））がワーク鍵Ｋｗで復号化され、この第一暗号鍵関連情報（Ｅ（ＥＣＭ．Ｋｗ））に含まれているスクランブル鍵ＫＳおよびハッシュ値Ｈ（Ｍｍｉ）が取得される。ハッシュ関数演算部２７で、送信側のコンテンツ送信装置１に備えられているハッシュ関数と同様のハッシュ関数で、利用条件情報Ｍｍｉが演算され、比較用ハッシュ値Ｈ（Ｍｍｉ）とされる。比較部３３で、ハッシュ値Ｈ（Ｍｍｉ）と比較用ハッシュ値Ｈ（Ｍｍｉ）とが比較される。また、利用判定部６３で利用条件情報Ｍｍｉの各条件を満たしているかどうかが判定される。これらの比較結果および判定結果に基づき、送出制御部３５で、スクランブル鍵ＫＳの送出が制御される。その後、デスクランブル部３７で、暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））がスクランブル鍵で復号化され、ＭＰＥＧ２デコード部３９でデコードされ、映像音声Ｍ

ａｖ（コンテンツ）として出力される。

【００８３】

このため、多重暗号化コンテンツに多重化されているハッシュ値Ｈ（Ｍｍｉ）と、送信側のハッシュ関数演算部１１に備えられるハッシュ関数と同様のハッシュ関数で利用条件情報Ｍｍｉが演算されて得られた比較用ハッシュ値Ｈ（Ｍｍｉ）とが比較され、この比較結果と、利用判定部６３の判定結果とに基づいて、映像音声Ｍａｖ（コンテンツ）が利用可能かどうかを判定することができる。

【００８４】

つまり、比較結果により、多重化されていたハッシュ値Ｈ（Ｍｍｉ）と演算して得られた比較用ハッシュ値Ｈ（Ｍｍｉ）とが一致した場合、利用条件情報Ｍｍｉが改ざんされていないことになり、映像音声Ｍａｖ（コンテンツ）の利用が許可される。また、多重化されていたハッシュ値Ｈ（Ｍｍｉ）と受信側で演算したハッシュ値Ｈ（Ｍｍｉ）とが一致しない場合、利用条件情報Ｍｍｉが改ざんされたことになり、映像音声Ｍａｖ（コンテンツ）の利用が不許可とされる。さらに、利用判定部６３による利用条件情報Ｍｍｉの判定結果に基づき映像音声Ｍａｖ（コンテンツ）が利用可能かどうか判定される。

【００８５】

これにより、映像音声Ｍａｖ（コンテンツ）の不正コピーの防止、または、不正なコピー制御情報を含む映像音声Ｍａｖ（コンテンツ）の生成を防止することができる。さらに、送信側の映像音声Ｍａｖ（コンテンツ）の制作者（放送事業者）の意図に応じて、利用条件情報Ｍｍｉを設定することで、受信側において、利用条件情報Ｍｍｉに基づいた映像音声Ｍａｖ（コンテンツ）の利用（再生）を実現することができる。

【００８６】

（コンテンツ送信装置の動作：第二の実施の形態）

次に、図８に示すフローチャートを参照して、図６に示したコンテンツ送信装置１Ａの動作を説明する。

まず、コンテンツ送信装置１ＡのＭＰＥＧ２エンコード部３に映像音声Ｍａｖ（コンテンツ）が入力され、このＭＰＥＧ２エンコード部３で映像音声Ｍａｖ（コンテンツ）がエンコードされて、ＭＰＥＧ２形式の映像音声コンテンツストリーム（ＴＳ）とされスクランブル部５へ出力される（Ｓ３１）。

【００８７】

続いて、スクランブル部５で映像音声コンテンツストリーム（ＴＳ）がスクランブル鍵ＫＳでスクランブルされて、暗号化コンテンツ（Ｅ（Ｍａｖ，ＫＳ））とされ、多重化部１３へ出力される（Ｓ３２）。このスクランブル部５で使用されたスクランブル鍵ＫＳに当該スクランブル鍵ＫＳに関する情報が付加されて、スクランブル鍵ＫＳを含む関連情報とされ、このスクランブル鍵ＫＳを含む関連情報がＥＣＭ生成部７に入力される。

【００８８】

また、マークアップ記述言語型利用条件情報Ｍｍｉ生成部５１で利用条件情報Ｍｍｉが生成され、この利用条件情報Ｍｍｉがハッシュ関数演算部１１へ出力されると共に、多重化部１３へ出力される（Ｓ３３）。なお、利用条件情報Ｍｍｉは、コンテンツ送信装置１Ａの所有者（または使用者、ユーザ）であるコンテンツ制作者、放送事業者の意図の応じて各条件が設定されて、この条件を盛り込んだものがマークアップ記述言語型利用条件情報Ｍｍｉ生成部５１で生成される。

【００８９】

すると、ハッシュ関数演算部１１で利用条件情報Ｍｍｉが当該ハッシュ関数演算部１１に備えられているハッシュ関数によって演算され、ハッシュ値Ｈ（Ｍｍｉ）とされてＥＣＭ生成部７へ出力される（Ｓ３４）。

【００９０】

そして、ＥＣＭ生成部７で、スクランブル鍵ＫＳを含む関連情報とハッシュ値Ｈ（Ｍｍｉ）とがワーク鍵Ｋｗで暗号化され、第一暗号鍵関連情報（Ｅ（ＥＣＭ，Ｋｗ））とされて多重化部１３に出力される（Ｓ３５）。その後、多重化部１３で暗号化コンテンツ（Ｅ（

Ｍａｖ．ＫＳ））、第一暗号鍵関連情報（Ｅ（ＥＣＭ．Ｋｗ））および利用条件情報Ｍｍｌが多重化され、多重暗号化コンテンツとされて、送出される（Ｓ３６）。

【００９１】

（コンテンツ受信装置の動作：第二の実施の形態）

次に、図９、図１０に示すフローチャートを参照して、図７に示したコンテンツ受信装置２１Ａの動作を説明する。なお、このコンテンツ受信装置２１Ａの動作の説明では、送信側のコンテンツ送信装置１Ａから送信された多重暗号化コンテンツを受信した後、利用条件情報Ｍｍｌが改ざんされているか否かにより、映像音声Ｍａｖ（コンテンツ）を再生するまでの概略を説明したものである。また、このコンテンツ受信装置２１Ａの動作の説明では、多重暗号化コンテンツを復号化またはデスクランブルにかかる情報のみに言及して説明している。

【００９２】

送信側のコンテンツ送信装置１Ａから送出された多重暗号化コンテンツが、コンテンツ受信装置２１Ａの受信分離部２３で受信される（Ｓ４１）。すると、受信分離部２３で多重暗号化コンテンツが分離され、暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））がデスクランブル部３７へ、ＤＳＭ－ＣＣデータカルーセル（利用条件情報Ｍｍｌ）が利用条件情報Ｍｍｌ抽出部６１へ、第一暗号鍵関連情報（Ｅ（ＥＣＭ．Ｋｗ））がＥＣＭ解析部３１へ出力される（Ｓ４２）。

【００９３】

そして、利用条件情報Ｍｍｌ抽出部６１で利用条件情報Ｍｍｌが抽出され、ハッシュ関数演算部２７、利用判定部６３および外部の蓄積装置（図示せず）等へ出力される（Ｓ４３）。すると、ハッシュ関数演算部２７で利用条件情報Ｍｍｌがハッシュ関数で演算され、比較用ハッシュ値Ｈ（Ｍｍｌ）が生成され、比較部３３へ出力される（Ｓ４４）。また、ＥＣＭ解析部３１で第一暗号鍵関連情報（Ｅ（ＥＣＭ．Ｋｗ））がワーク鍵Ｋｗで復号化され、ハッシュ値Ｈ（Ｍｍｌ）およびスクランブル鍵ＫＳが取得され、ハッシュ値Ｈ（Ｍｍｌ）が比較部３３へ出力されると共に、スクランブル鍵ＫＳが送出制御部３５へ出力される（Ｓ４５）。これより図１０を参照する。

【００９４】

そして、利用判定部６３で暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））つまり映像音声Ｍａｖが利用可能かどうか（各条件を満たしているかどうか）が判定される（Ｓ４６）。この利用判定部６３で暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））つまり映像音声Ｍａｖが利用可能であると判定された場合（Ｓ４６、Ｙｅｓ）、利用判定部６３から映像音声Ｍａｖ利用許可信号（図中、許可信号）が送出制御部３５へ出力される（Ｓ４７）。

【００９５】

さらに、比較部３３でハッシュ値Ｈ（Ｍｍｌ）と比較用ハッシュ値Ｈ（Ｍｍｌ）とが比較され、一致するか否かが判定される（Ｓ４８）。つまり、このＳ４８にて、比較部３３でハッシュ値Ｈ（Ｍｍｌ）と比較用ハッシュ値Ｈ（Ｍｍｌ）とが比較された結果（比較結果）によって、利用条件情報Ｍｍｌが改ざんされたか否かが判断できる。すなわち、比較結果が一致していれば、改ざんされていないと判断でき、一致していなければ、改ざんされていると判断できる。

【００９６】

この比較部３３でハッシュ値Ｈ（Ｍｍｌ）と比較用ハッシュ値Ｈ（Ｍｍｌ）とが一致すると判定された場合（Ｓ４８、Ｙｅｓ）、比較部３３からスクランブル鍵ＫＳ送出許可信号（図中、許可信号）が送出制御部３５へ出力される（Ｓ４９）。送出制御部３５で、スクランブル鍵ＫＳ送出許可信号に基づいて、スクランブル鍵ＫＳがデスクランブル部３７へ出力される（Ｓ５０）。デスクランブル部３７で暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））がデスクランブルされ、ＭＰＥＧ２形式の映像音声コンテンツストリーム（ＴＳ）が得られ、ＭＰＥＧ２デコード部３９に出力される（Ｓ５１）。ＭＰＥＧ２デコード部３９で、ＭＰＥＧ２形式の映像音声コンテンツストリーム（ＴＳ）がデコードされ映像音声Ｍａｖ（コンテンツ）が出力される（Ｓ５２）。

【００９７】
また、Ｓ４６にて、利用判定部６３で暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））つまり映像音声Ｍａｖが利用可能であると判定されない場合（Ｓ４６、Ｎｏ）、利用判定部６３から映像音声Ｍａｖ利用不可信号（図中、不可信号）が送出制御部３５へ出力される（Ｓ５３）。暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））つまり映像音声Ｍａｖを再生できない旨（利用条件情報Ｍｍｌによる）のメッセージが図示を省力した表示部に表示される（Ｓ５４）。
【００９８】
また、Ｓ４８にて、比較部３３でハッシュ値Ｈ（Ｍｍｌ）と比較用ハッシュ値Ｈ（Ｍｍｌ）とが一致しないと判定された場合（Ｓ４８、Ｎｏ）、比較部３３からスクランブル鍵ＫＳ送出不可信号（図中、不可信号）が送出制御部３５へ出力され（Ｓ５５）、暗号化コンテンツ（Ｅ（Ｍａｖ．ＫＳ））つまり映像音声Ｍａｖを再生できない旨のメッセージが図示を省力した表示部に表示される（Ｓ５６）。
【００９９】
（デジタルコピー制御記述子について）
最後に、デジタル制御記述子について説明する。図１１は、デジタルコピー制御記述子（データテーブル）の具体的な例を示した図である。この図１１に示したように、デジタルコピー制御記述子は、デジタル記録機器におけるコピー世代を制御する情報および最大伝送レートの記述をしたものであり、先頭（図中左側）から８ｂｉｔの「記述子タグ」、８ｂｉｔの「記述子長」、２ｂｉｔの「デジタルコピー制御情報」、１ｂｉｔの「最大伝送レートフラグ」、１ｂｉｔの「コンポーネント制御フラグ」、２ｂｉｔの「コピー制御タイプ」および２ｂｉｔの「ＡＰＳ制御データ」を含んでいる。
【０１００】
「記述子タグ」は、デジタルコピー制御記述子の始まりを示すと共に、記述子の識別するためのものである。「記述子長」は、記述子の長さ（領域）を示したものである。
【０１０１】
「デジタルコピー制御情報」は、デジタルコンテンツの複写（コピー）を制御する情報であり、「コピー不可」「コピー一世代」「コピー自由」等に分けられている。「最大伝送レートフラグ」は、最大伝送レートを識別するためのフラグである。
【０１０２】
「コンポーネント制御フラグ」は、コンポーネント（映像、音声、データ等）毎にコピー制御情報が付与されている場合に１となるもので、この場合、コンポーネント毎にコピー制御情報が記述されている。「ＡＰＳ制御データ」は、ＡＰＳ（Ａｎａｌｏｇ　Ｐｒｏｔｅｃｔｉｏｎ　ＳＹＳｔｅｍ）を制御するための情報である。
【０１０３】
以上、一実施形態に基づいて本発明を説明したが、本発明はこれに限定されるものではない。
【０１０４】
例えば、コンテンツ送信装置１、１Ａ、コンテンツ受信装置２１、２１Ａの各構成の処理を一つずつの過程ととらえたコンテンツ送信方法、コンテンツ受信方法とみなすことや、各構成の処理を汎用のコンピュータ言語で記述したコンテンツ送信プログラム、コンテンツ受信プログラムとみなすこともできる。
【０１０５】
これらの場合、コンテンツ送信装置１、１Ａ、コンテンツ受信装置２１、２１Ａのそれぞれと同様の効果を得ることができる。また、コンテンツ送信プログラムおよびコンテンツ受信プログラムとした場合には、これらのプログラムを記録媒体等に記録して流通させることもできる。
【０１０６】
【発明の効果】
請求項１、２、４記載の発明によれば、コンテンツが第一暗号鍵で暗号化され、暗号化コ

ンテンツとされる。コピー制御情報が所定関数で演算され、関数演算情報に加工される。そして、第一暗号鍵および関数演算情報が第二暗号鍵で暗号化され、第一暗号鍵関連情報とされる。その後、暗号化コンテンツ、コピー制御情報および第一暗号鍵関連情報が多重化され送出される。このため、受信側にて、多重暗号化コンテンツに多重化されている関数演算情報と、受信側で送信側の所定関数と同様の所定関数でコピー制御情報が演算されて得られたものとが比較されれば、この比較結果に基づいて、コンテンツが利用可能かどうかを判定することができる。これにより、コンテンツの不正コピーの防止、または、不正なコピー制御情報を含むコンテンツの生成を防止することができる。

【０１０７】

請求項８記載の発明によれば、コンテンツが第一暗号鍵で暗号化され、暗号化コンテンツとされる。また、コピー制御情報を含む利用条件情報が所定関数で演算され、関数演算情報に加工される。そして、第一暗号鍵および関数演算情報が第二暗号鍵で暗号化され、第一暗号鍵関連情報とされる。その後、暗号化コンテンツ、利用条件情報および第一暗号鍵関連情報が多重化され送出される。このため、受信側にて、多重暗号化コンテンツに多重化されている関数演算情報と、受信側で送信側に備えられる所定関数と同様の所定関数で利用条件情報が演算されて得られたものとが比較され、さらに利用条件情報に基づいて、暗号化コンテンツを復号化可能かが判定されれば、これら比較結果および判定結果に基づいて、コンテンツが利用可能かどうかを判定することができる。これにより、コンテンツの不正コピーの防止、または、不正なコピー制御情報を含むコンテンツの生成を防止することができる。さらに、コンテンツの制作者（放送事業者）の意図に応じて、利用条件情報を設定することで、受信側において、利用条件情報に基づいたコンテンツの利用（再生）を実現することができる。

【０１０８】

請求項５、６、８記載の発明によれば、受信された多重暗号化コンテンツが暗号化コンテンツおよびコピー制御情報と、第一暗号鍵関連情報とに分離される。続いて、第一暗号鍵関連情報が第二暗号鍵で復号化され、この第一暗号鍵関連情報に含まれている第一暗号鍵および関数演算情報が取得される。送信側に備えられている所定関数と同様の所定関数で、コピー制御情報が演算され、比較用関数演算情報とされる。関数演算情報と比較用関数演算情報とが比較され、この比較結果に基づき、第一暗号鍵の送出が制御される。その後、暗号化コンテンツが第一暗号鍵で復号化されて出力される。このため、多重暗号化コンテンツに多重化されている関数演算情報と、送信側に備えられる所定関数と同様の所定関数でコピー制御情報が演算されて得られたものとが比較され、この比較結果に基づいて、コンテンツが利用可能かどうかを判定することができる。これにより、コンテンツの不正コピーの防止、または、不正なコピー制御情報を含むコンテンツの生成を防止することができる。

【０１０９】

請求項７記載の発明によれば、受信された多重暗号化コンテンツが暗号化コンテンツと、利用条件情報と、第一暗号鍵関連情報とに分離される。続いて、第一暗号鍵関連情報が第二暗号鍵で復号化され、この第一暗号鍵関連情報に含まれている第一暗号鍵および関数演算情報が取得される。送信側に備えられている所定関数と同様の所定関数で、利用条件情報が演算され、比較用関数演算情報とされる。関数演算情報と比較用関数演算情報とが比較され、暗号化コンテンツが復号化可能か判定され、これら比較結果、判定結果に基づき、第一暗号鍵の送出が制御される。その後、暗号化コンテンツが第一暗号鍵で復号化されて出力される。このため、多重暗号化コンテンツに多重化されている関数演算情報と、送信側に備えられる所定関数と同様の所定関数で利用条件情報が演算されて得られたものとが比較され、この比較結果と、利用条件情報に基づいて、暗号化コンテンツを復号化可能かが判定され判定結果とに基づいて、コンテンツが利用可能かどうかを判定することができる。これにより、コンテンツの不正コピーの防止、または、不正なコピー制御情報を含むコンテンツの生成を防止することができる。さらに、送信側のコンテンツの制作者（放送事業者）の意図に応じた利用条件情報に基づいたコンテンツの利用（再生）を実現する

ことができる。

【図面の簡単な説明】

【図１】本発明による一実施の形態であるコンテンツ送信装置のブロック図である。

【図２】本発明による一実施の形態であるコンテンツ受信装置のブロック図である。

【図３】図１に示したコンテンツ送信装置の動作を説明したフローチャートである。

【図４】図２に示したコンテンツ受信装置の動作を説明したフローチャートである。

【図５】図２に示したコンテンツ受信装置の動作を説明したフローチャートである（図４の続き）。

【図６】本発明による他の実施の形態であるコンテンツ送信装置のブロック図である。

【図７】本発明による他の実施の形態であるコンテンツ受信装置のブロック図である。

【図８】図６に示したコンテンツ送信装置の動作を説明したフローチャートである。

【図９】図７に示したコンテンツ受信装置の動作を説明したフローチャートである。

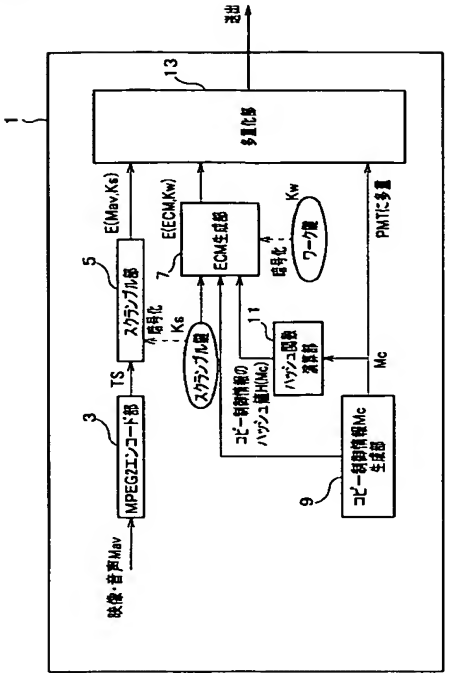
【図１０】図７に示したコンテンツ受信装置の動作を説明したフローチャートである（図９の続き）。

【図１１】デジタルコピー制御記述子の例を説明した図である。

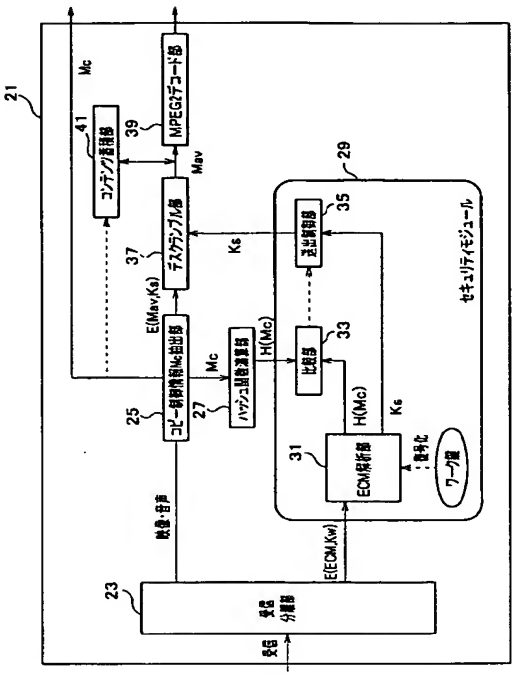
【符号の説明】

１、１Ａ	コンテンツ送信装置
３	ＭＰＥＧ２エンコード部
５	スクランブル部
７	ＥＣＭ生成部
９	コピー制御情報Ｍｃ生成部
１１、２７	ハッシュ関数演算部
１３	多重化部
２１、２１Ａ	コンテンツ受信装置
２３	受信分離部
２５	コピー制御情報Ｍｃ抽出部
２９、２９Ａ	セキュリティモジュール
３１	ＥＣＭ解析部
３３	比較部
３５	送出制御部
３７	デスクランブル部
３９	ＭＰＥＧ２デコード部
４１	コンテンツ蓄積部

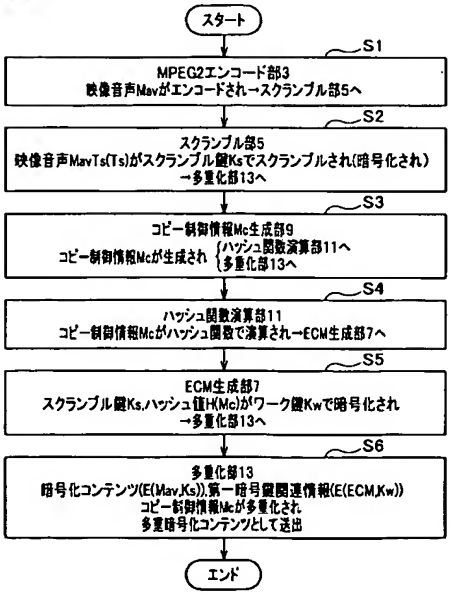
【図１】


送信
1
13
多重化部
E(Mav,Ks)
E(ECM,Kw)
ECM生成部
Kw
ワード鍵
暗号化
PMTに多重
5
スクランブル部
7
暗号化
Ks
スクランブル鍵
11
ハッシュ関数演算部
コピー制御情報のハッシュ値H(Mc)
TS
Mc
3
MPEG2エンコード部
コピー制御情報Mc生成部
9
映像・音声Mav

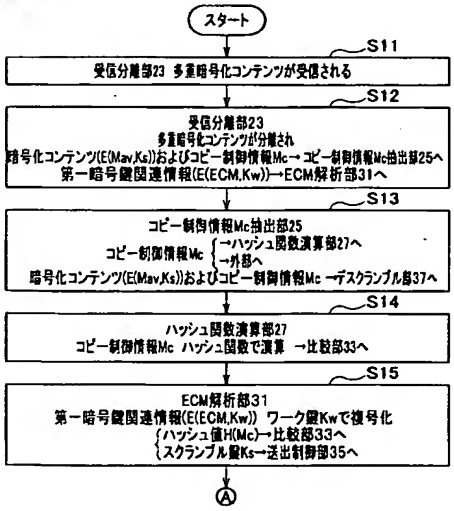
【図２】


21
Mc
MPEG2デコード部
41
コンテンツ情報部
39
Mav
29
35
送出制御部
37
デスクランブル部
Ks
セキュリティモジュール
E(Mav,Ks)
コピー制御情報Mc抽出部
Mc
ハッシュ関数演算部
H(Mc)
33
比較部
25
27
31
ECM解析部
暗号化
ワード鍵
映像・音声
E(ECM,Kw)
23
受信分離部
受信

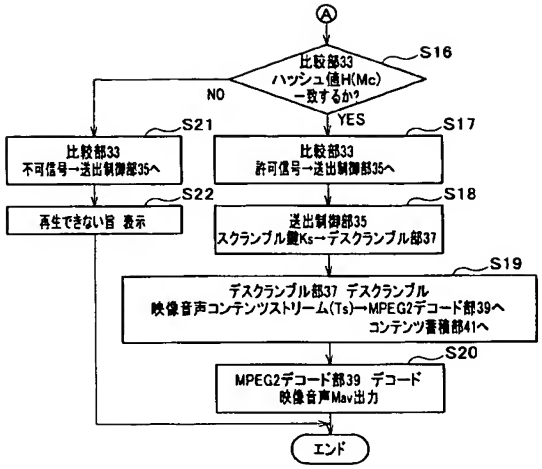
【図３】


スタート
S1
MPEG2エンコード部3
映像音声Mavがエンコードされ→スクランブル部5へ
S2
スクランブル部5
映像音声MavTs(Ts)がスクランブル鍵Ksでスクランブルされ(暗号化され)
→多重化部13へ
S3
コピー制御情報Mc生成部9
コピー制御情報Mcが生成され {→ハッシュ関数演算部11へ / →多重化部13へ}
S4
ハッシュ関数演算部11
コピー制御情報Mcがハッシュ関数で演算され→ECM生成部7へ
S5
ECM生成部7
スクランブル鍵Ks,ハッシュ値H(Mc)がワード鍵Kwで暗号化され
→多重化部13へ
S6
多重化部13
暗号化コンテンツ(E(Mav,Ks))第一暗号鍵関連情報(E(ECM,Kw))
コピー制御情報Mcが多重化され
多重暗号化コンテンツとして送出
エンド

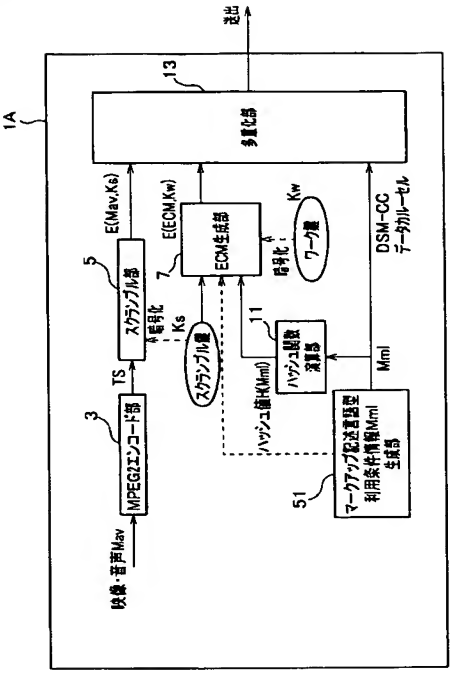
【図４】


スタート
S11
受信分離部23 多重暗号化コンテンツが受信される
S12
受信分離部23
多重暗号化コンテンツが分離され
暗号化コンテンツ(E(Mav,Ks))およびコピー制御情報Mc→コピー制御情報Mc抽出部25へ
第一暗号鍵関連情報(E(ECM,Kw))→ECM解析部31へ
S13
コピー制御情報Mc抽出部25
コピー制御情報Mc {→ハッシュ関数演算部27へ / →外部へ}
暗号化コンテンツ(E(Mav,Ks))およびコピー制御情報Mc →デスクランブル部37へ
S14
ハッシュ関数演算部27
コピー制御情報Mc ハッシュ関数で演算 →比較部33へ
S15
ECM解析部31
第一暗号鍵関連情報(E(ECM,Kw)) ワード鍵Kwで復号化
{ハッシュ値H(Mc)→比較部33へ / スクランブル鍵Ks→送出制御部35へ}
Ⓐ

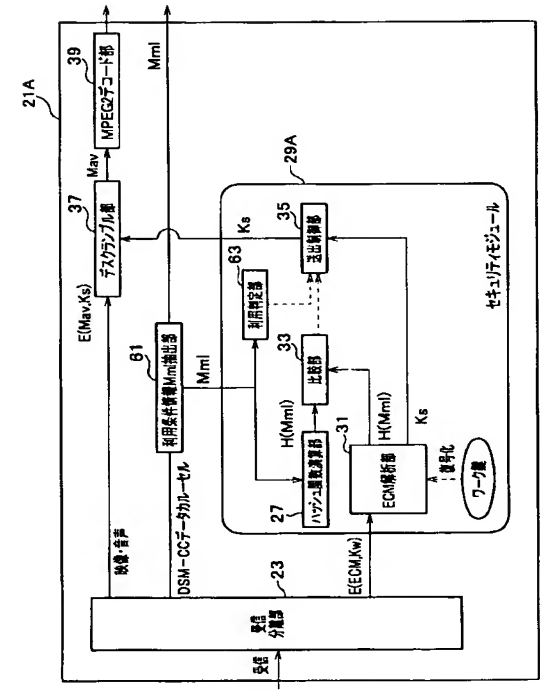
【図５】


Ⓐ
比較部33
ハッシュ値H(Mc)
一致するか?
S16
NO
YES
S21
比較部33
不可信号→送出制御部35へ
S17
比較部33
許可信号→送出制御部35へ
S22
再生できない旨 表示
S18
送出制御部35
スクランブル鍵Ks→デスクランブル部37
S19
デスクランブル部37 デスクランブル
映像音声コンテンツストリーム(Ts)→MPEG2デコード部39へ
コンテンツ蓄積部41へ
S20
MPEG2デコード部39 デコード
映像音声Mav出力
エンド

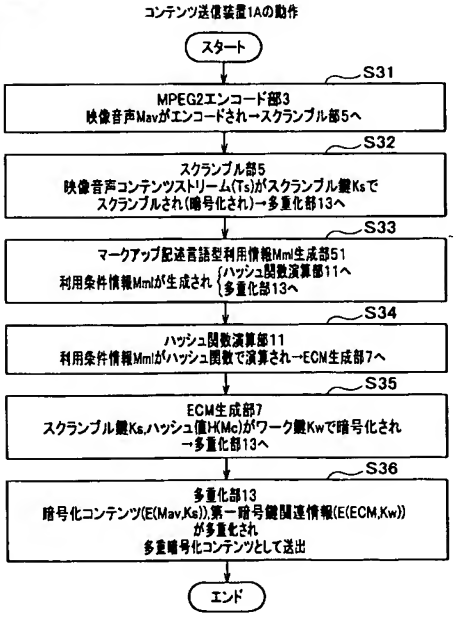
【図６】


送出
1A
13
多重化部
E(Mav,Ks)
E(ECM,Kw)
Kw
ワード鍵
DSM-CC
データカルーセル
5
スクランブル部
暗号化
Ks
スクランブル鍵
7
ECM生成部
暗号化
11
ハッシュ関数
演算部
ハッシュ値H(Mml)
Mml
TS
3
MPEG2エンコード部
映像・音声Mav
51
マークアップ記述言語型
利用条件情報Mml
生成部

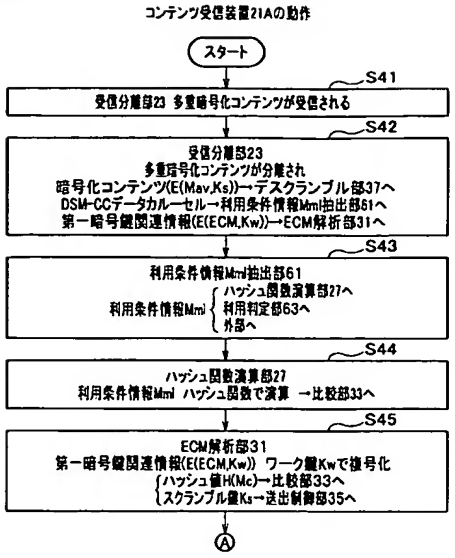
【図７】


21A
39
MPEG2デコード部
Mml
Mav
29A
37
デスクランブル鍵
Ks
35
送出制御部
E(Mav,Ks)
63
利用許可部
61
利用条件情報Mml抽出部
Mml
33
比較部
セキュリティモジュール
H(Mml)
31
H(Mml)
Ks
ハッシュ関数演算部
27
ECM構築部
暗号化
ワード鍵
映像・音声
DSM-CCデータカルーセル
23
E(ECM,Kw)
受信
分離部
受信

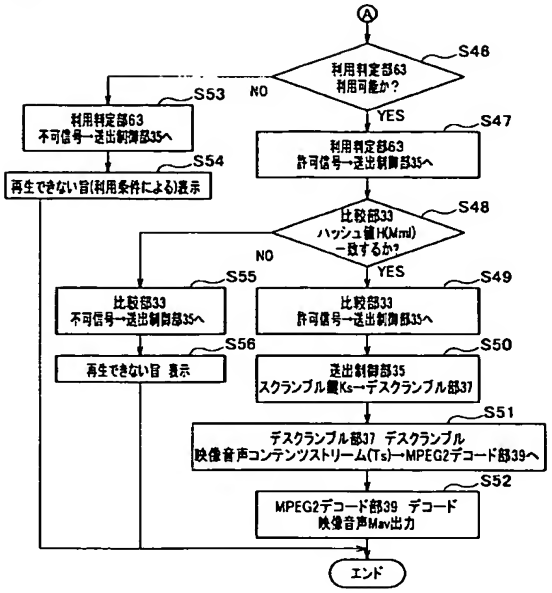
【図８】


コンテンツ送信装置1Aの動作
スタート
S31
MPEG2エンコード部3
映像音声Mavがエンコードされ→スクランブル部5へ
S32
スクランブル部5
映像音声コンテンツストリーム(Ts)がスクランブル鍵Ksで
スクランブルされ(暗号化され)→多重化部13へ
S33
マークアップ記述言語型利用情報Mml生成部51
利用条件情報Mmlが生成され
ハッシュ関数演算部11へ
多重化部13へ
S34
ハッシュ関数演算部11
利用条件情報Mmlがハッシュ関数で演算され→ECM生成部7へ
S35
ECM生成部7
スクランブル鍵Ks,ハッシュ値H(Mc)がワード鍵Kwで暗号化され
→多重化部13へ
S36
多重化部13
暗号化コンテンツ(E(Mav,Ks)),第一暗号鍵関連情報(E(ECM,Kw))
が多重化され
多重暗号化コンテンツとして送出
エンド

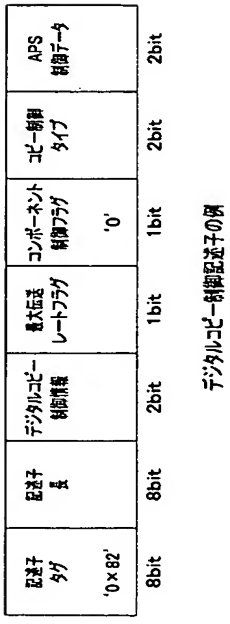
【図９】


コンテンツ受信装置21Aの動作
スタート
S41
受信分離部23 多重暗号化コンテンツが受信される
S42
受信分離部23
多重暗号化コンテンツが分離され
暗号化コンテンツ(E(Mav,Ks))→デスクランブル部37へ
DSM-CCデータカルーセル→利用条件情報Mml抽出部61へ
第一暗号鍵関連情報(E(ECM,Kw))→ECM解析部31へ
S43
利用条件情報Mml抽出部61
利用条件情報Mml { ハッシュ関数演算部27へ / 利用判定部63へ / 外部へ
S44
ハッシュ関数演算部27
利用条件情報Mml ハッシュ関数で演算 →比較部33へ
S45
ECM解析部31
第一暗号鍵関連情報(E(ECM,Kw)) ワーク鍵Kwで復号化
{ハッシュ値H(Mc)→比較部33へ
{スクランブル鍵Ks→送出制御部35へ
A

【図１０】


A
S46
利用判定部63
利用可能か?
NO
YES
S53
利用判定部63
不可信号→送出制御部35へ
S47
利用判定部63
許可信号→送出制御部35へ
S54
再生できない旨(利用条件による)表示
S48
比較部33
ハッシュ値H(Mml)
一致するか?
NO
YES
S55
比較部33
不可信号→送出制御部35へ
S49
比較部33
許可信号→送出制御部35へ
S56
再生できない旨 表示
S50
送出制御部35
スクランブル鍵Ks→デスクランブル部37
S51
デスクランブル部37 デスクランブル
映像音声コンテンツストリーム(Ts)→MPEG2デコード部39へ
S52
MPEG2デコード部39 デコード
映像音声Mav出力
エンド

【図１１】


APS 制御データ 2bit
コピー制御タイプ 2bit
コンポーネント制御フラグ '0' 1bit
最大伝送レートフラグ 1bit
デジタルコピー制御情報 2bit
記述子長 8bit
記述子タグ '0×82' 8bit
デジタルコピー制御記述子の例

フロントページの続き

(72)発明者 桑岡 辰弥
東京都世田谷区砧一丁目１０番１１号 日本放送協会 放送技術研究所内

Ｆターム(参考) 5B017 AA06 BA09 BB10 CA16
5C064 BA01 BB02 BC06 BC17 BC22 BC23 BD02 BD08 BD09 CA14
CB01 CC04
5J104 AA08 AA12 AA16 BA04 EA04 EA15 NA02 NA03 NA12 PA07